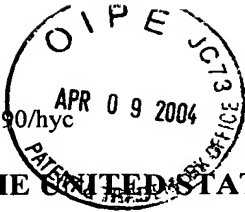


Docket No. 245395US90/hyc



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takehiro NAKAYAMA, et al.

GAU:

SERIAL NO: 10/705,818

EXAMINER:

FILED: November 13, 2003

FOR: COMMUNICATION TERMINAL, VALUE ENTITY PROVIDING SERVER, APPLICATION DELIVERY SERVER, ELECTRONIC PROCUREMENT SUPPORTING METHOD, AND ELECTRONIC PROCUREMENT SUPPORTING PROGRAM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2002-338558	November 21, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Bradley D. Lytle

Registration No. 40,073

Joseph A. Scafetta, Jr.  
Registration No. 26, 803

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 2 年 1 1 月 2 1 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 2 - 3 3 8 5 5 8  
Application Number:  
[ST. 10/C]:                      [ J P 2 0 0 2 - 3 3 8 5 5 8 ]

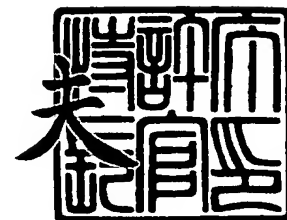
出      願      人                      株式会社エヌ・ティ・ティ・ドコモ  
Applicant(s):



特許庁長官  
Commissioner,  
Japan Patent Office

2 0 0 3 年 1 1 月 1 9 日

今 井 康



【書類名】 特許願

【整理番号】 14-0409

【提出日】 平成14年11月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 15/00

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 中山 雄大

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 中野 博隆

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100088155

【弁理士】

【氏名又は名称】 長谷川 芳樹

【選任した代理人】

【識別番号】 100092657

【弁理士】

【氏名又は名称】 寺崎 史朗

【選任した代理人】

【識別番号】 100114270

【弁理士】

【氏名又は名称】 黒川 朋也

## 【選任した代理人】

【識別番号】 100108213

【弁理士】

【氏名又は名称】 阿部 豊隆

## 【選任した代理人】

【識別番号】 100113549

【弁理士】

【氏名又は名称】 鈴木 守

## 【手数料の表示】

【予納台帳番号】 014708

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信端末、価値実体提供サーバ、アプリケーション配信サーバ、電子購買支援システム、電子購買支援方法、及び電子購買支援プログラム

【特許請求の範囲】

【請求項 1】

特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得手段と、  
前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信手段と、  
前記公開鍵を使用して前記アプリケーションを検証する検証手段と、  
前記検証手段による前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転手段と  
を備えることを特徴とする通信端末。

【請求項 2】

前記検証手段は、前記受信手段により前記アプリケーションが受信されたことを契機として前記アプリケーションの検証を開始し、  
前記検証手段による前記アプリケーションの検証が成功したことを契機として前記アプリケーションを起動する起動手段  
を更に備えることを特徴とする請求項 1 に記載の通信端末。

【請求項 3】

前記受信手段により前記アプリケーションが受信された時点から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段  
を更に備えることを特徴とする請求項 1 又は 2 に記載の通信端末。

【請求項 4】

前記受信手段により前記アプリケーションが受信された後に、当該アプリケーションの送信元との通信が切断された場合に、通信切断時から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段  
を更に備えることを特徴とする請求項 1 又は 2 に記載の通信端末。

【請求項 5】

請求項 1 に記載の通信端末に対して、セルラーネットワークを経由して、特定

の秘密鍵に対応する公開鍵が添付された価値実体を提供する提供手段を備えることを特徴とする価値実体提供サーバ。

【請求項 6】

前記提供手段は、価値実体の提供に先立って、当該価値実体とは別に前記公開鍵を前記通信端末に送信することを特徴とする請求項 5 に記載の価値実体提供サーバ。

【請求項 7】

前記公開鍵は、セルラーネットワークを経由して複数の端末からアクセス可能なサーバ上に公開されていることを特徴とする請求項 5 に記載の価値実体提供サーバ。

【請求項 8】

前記提供手段により前記価値実体が提供される前に、前記通信端末のインテグリティを検証する第 2 検証手段を更に備えることを特徴とする請求項 5 に記載の価値実体提供サーバ。

【請求項 9】

請求項 1 に記載の通信端末に対して、アドホックネットワークを経由して、前記アプリケーションを送信するアプリケーション送信手段と、

前記通信端末の移転手段により移転された価値実体を、前記アドホックネットワークを経由して取得する価値実体取得手段とを備えることを特徴とするアプリケーション配信サーバ。

【請求項 1 0】

前記価値実体取得手段により前記価値実体が取得された場合に、当該価値実体が受領された旨が電子的に表現された領収書データを、前記アドホックネットワークを経由して前記通信端末に送信する領収書送信手段を更に備えることを特徴とする請求項 9 に記載のアプリケーション配信サーバ。

【請求項 1 1】

前記送信手段により前記アプリケーションが送信される前に、前記通信端末のインテグリティを検証する第 3 検証手段を更に備えることを特徴とする請求項 9 に記載のアプリケーション配信サーバ。

**【請求項 1 2】**

請求項 1 に記載の通信端末と、請求項 5 に記載の価値実体提供サーバと、請求項 9 に記載のアプリケーション配信サーバとを備えて構成され、

前記通信端末は、前記価値実体提供サーバから提供された価値実体を取得すると共に、前記アプリケーション配信サーバから受信されたアプリケーションを使用して前記価値実体を移転することを特徴とする電子購買支援システム。

**【請求項 1 3】**

通信端末が、取得手段により、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得ステップと、

前記通信端末が、受信手段により、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信ステップと、

前記通信端末が、検証手段により、前記公開鍵を使用して前記アプリケーションを検証する検証ステップと、

前記通信端末が、前記検証手段による前記アプリケーションの検証が成功した場合に、移転手段により、当該アプリケーションを使用して前記価値実体を移転する移転ステップと

を含むことを特徴とする電子購買支援方法。

**【請求項 1 4】**

通信端末により実行可能な電子購買支援プログラムにおいて、

特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得機能と、

前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信機能と、

前記公開鍵を使用して前記アプリケーションを検証する検証機能と、

前記検証機能による、前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転機能と

を前記通信端末に実現させることを特徴とする電子購買支援プログラム。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明は、通信端末、価値実体提供サーバ、アプリケーション配信サーバ、電子購買支援システム、電子購買支援方法、及び電子購買支援プログラムに関する。

#### 【 0 0 0 2 】

##### 【従来の技術】

近年、携帯電話などの携帯型通信端末（以下、「携帯端末」と記す。）の普及や無線通信速度の高速化に伴い、インターネット等のネットワークを介して、携帯端末がサーバ装置から所望のコンテンツデータを取得することが可能な情報通信システムが実用化されている。このようなシステムを利用した電子商取引においては、クレジットカードや現金を使用しない代金支払い手段として、価値実体が使用されることがある。

#### 【 0 0 0 3 】

価値実体とは、電子化されたデータで何らかの経済価値が表現（化体）されたものである。価値実体は、電子バリューと称されることもあり、例えば、貨幣価値が表現された電子マネー（電子貨幣或いは電子通貨などと称されることもある。）の他に、プリペイド方式で提供される電子チケット等がある。電子チケットには、例えば、図書券、回数券、乗車券などの価値が表現されている。

#### 【 0 0 0 4 】

かかる価値実体を安全に流通する方法としては、例えば、耐タンパー性を有する I C（Integrated Circuit）カードに充填（チャージ）された価値実体を、専用のカードリーダを用いて移転させる技術が提案されている（例えば、非特許文献 1 参照。）。

#### 【 0 0 0 5 】

しかし、I C カードは、携帯性や可搬性に優れている反面、例えば、以下に示す様な問題点もある。

1. ユーザインタフェースをもたないので、別体の表示装置に接続しなければ、価値実体の残量を確認できない。
2. アプリケーションを実装できないので、ユーザに対して、電子購買活動をグラフィカルにナビゲートできない。



3. 通信手段をもたないので、別体の通信装置に接続しなければ、価値実体を充填できない。

【0 0 0 6】

一方で、携帯性に優れ、かつ、上記問題点を有さない携帯端末として、携帯電話がある。携帯電話は、表示装置などのユーザインタフェースを有すると共に、アプリケーションを実装可能である。また、無線通信手段により、外部のサーバ装置から価値実体を充填することもできる。

【0 0 0 7】

携帯電話がアプリケーションを取得する際には、セルラーネットワーク経由でダウンロードするのが一般的である。セルラーネットワークとは、通信事業者が運営する無線基地局などのインフラストラクチャを利用した無線公衆網である。しかし、アプリケーションの中には、安全性が保証されていないものもあり、ダウンロードして実行した際に、携帯電話に危害が及ぶ場合がある。

【0 0 0 8】

かかる懸念を解消するために、セルラーネットワークでは、携帯電話内の特定のメモリ領域に対するアプリケーションのアクセスを制限すると共に、アプリケーションを使用して通信できるサーバをその配信元に限定する、といった手法が採られている（例えば、非特許文献2 参照。）。

【0 0 0 9】

また、他のセルラーネットワークには、正規の作成元として認定された者により作成されたアプリケーションだけがW e b サイトからダウンロードできる仕様になっているものもある（例えば、非特許文献3 参照。）。

【0 0 1 0】

【非特許文献1】

「電子マネーを構成する情報セキュリティ技術と安全性評価」IMES Discussion Paper Series 98-J-26、1998年11月、日本銀行金融研究所

【非特許文献2】

i モード対応 J a v a コンテンツ開発ガイド 詳細編 第1. 1 版、平成13年5月14日、株式会社N T T ドコモ、[http://www.nttdocomo.co.jp/p\\_s/](http://www.nttdocomo.co.jp/p_s/)

imode/java/pdf/jguide010514.pdf

【非特許文献 3】

J - P H O N E J a v a アプリ開発ガイド Version 1.1.5, Nov.28  
, 2001、[http://www.dp.j-phone.com/file/j\\_java\\_dg115.pdf](http://www.dp.j-phone.com/file/j_java_dg115.pdf)

【0 0 1 1】

【発明が解決しようとする課題】

このように、上記従来技術では、セルラーネットワークにおける価値実体の流通の安全性を確保すべく、人手を掛けて安全性を検証したアプリケーションのみを流通させたり、携帯端末の通信相手を制限したりしている。しかしながら、これらの手法は、セルラーネットワークの利用を前提とするものであり、アドホックネットワークを経由して取得されたアプリケーションの使用を想定したものではなかった。

【0 0 1 2】

セルラーネットワークは、通信事業者の管理下にある、言わば閉じたネットワークであり、通信相手の認証が正確に行われる可能性が高い。このため、セルラーネットワークを利用する通信では、第三者が介入する恐れが低く、比較的安全である。これに対して、アドホックネットワークは、無線基地局などの特定のインフラストラクチャに依存せず携帯端末間で一時的に形成される、言わばオープンなネットワークである。したがって、アドホックネットワークから取得されたアプリケーションが、携帯端末に充填された価値実体にアクセスすることには危険の伴う可能性がある。

【0 0 1 3】

そこで、上記問題点に鑑みて、本発明は、アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことを課題とする。

【0 0 1 4】

【課題を解決するための手段】

上記課題を解決するために、本発明に係る通信端末は、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得手段と、前記秘密鍵によって電子

署名されたアプリケーションをアドホックネットワークを経由して受信する受信手段と、前記公開鍵を使用して前記アプリケーションを検証する検証手段と、前記検証手段による前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転手段とを備える。

#### 【0015】

本発明に係る価値実体提供サーバは、上述した通信端末に対して、セルラーネットワークを経由して、特定の秘密鍵に対応する公開鍵が添付された価値実体を提供する提供手段を備える。

#### 【0016】

本発明に係るアプリケーション配信サーバは、上述した通信端末に対して、アドホックネットワークを経由して、前記アプリケーションを送信するアプリケーション送信手段と、前記通信端末の移転手段により移転された価値実体を、前記アドホックネットワークを経由して取得する価値実体取得手段とを備える。

#### 【0017】

本発明に係る電子購買支援システムは、上述した通信端末と、上述した価値実体提供サーバと、上述したアプリケーション配信サーバとを備えて構成される。前記通信端末は、前記価値実体提供サーバから提供された価値実体を取得すると共に、前記アプリケーション配信サーバから受信されたアプリケーションを使用して前記価値実体を移転することを特徴とする電子購買支援システムを構築してもよい。

#### 【0018】

本発明に係る電子購買支援方法は、通信端末が、取得手段により、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得ステップと、前記通信端末が、受信手段により、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信ステップと、前記通信端末が、検証手段により、前記公開鍵を使用して前記アプリケーションを検証する検証ステップと、前記通信端末が、前記検証手段による前記アプリケーションの検証が成功した場合に、移転手段により、当該アプリケーションを使用して前記価値実体を移転する移転ステップとを含む。

## 【 0 0 1 9 】

本発明に係る電子購買支援プログラムは、通信端末により実行可能な電子購買支援プログラムにおいて、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得機能と、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信機能と、前記公開鍵を使用して前記アプリケーションを検証する検証機能と、前記検証機能による、前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転機能とを前記通信端末に実現させる。

## 【 0 0 2 0 】

これらの発明によれば、特定の秘密鍵に対応する公開鍵が添付された価値実体が価値実体提供サーバから通信端末に提供されると共に、前記秘密鍵によって電子署名されたアプリケーションがアドホックネットワークを経由してアプリケーション配信サーバから通信端末宛に送信される。前記アプリケーションは、前記公開鍵を使用して検証される。検証が成功した場合には、当該アプリケーションを使用して、前記価値実体の少なくとも一部が対価としてアプリケーション配信サーバに移転される。これにより、価値実体の提供元とアプリケーションへの署名元との同一性を確認した上で、価値実体に対するアプリケーションへのアクセスを許可することができる。したがって、通信事業者が介在しないアドホックネットワークを経由して取得されたアプリケーションを使用しても、安全かつ容易に価値実体の授受を行うことが可能となる。

## 【 0 0 2 1 】

本発明に係る通信端末において、前記検証手段は、前記受信手段により前記アプリケーションが受信されたことを契機として前記アプリケーションの検証を開始し、前記検証手段による前記アプリケーションの検証が成功したことを契機として前記アプリケーションを起動する起動手段を更に備えるものとしてもよい。

## 【 0 0 2 2 】

本発明によれば、アプリケーションは、受信されたことを契機として検証され、検証が成功したことを契機として起動される。これにより、受信されたアプリケーションが正規のものである場合には、通信端末のユーザからの指示を待たず

に、安全なアプリケーションが起動される。したがって、通信端末のユーザは、取得したアプリケーションを簡易迅速に使用することができる。

#### 【 0 0 2 3 】

本発明に係る通信端末において、前記受信手段により前記アプリケーションが受信された時点から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段を更に備えるものとしてもよい。

#### 【 0 0 2 4 】

本発明によれば、アプリケーションは、受信された時点から所定時間が経過したことを契機として削除される。これにより、通信端末のユーザからの指示を待たずに、アプリケーションが削除される。したがって、通信端末のユーザが、かかるアプリケーションを、該アプリケーションに適当でない電子商取引（例えばサービス内容の異なる電子商取引）に誤って使用すること等により、電子商取引に混乱が生じることがない。その結果、電子購買支援の信頼性が維持される。

#### 【 0 0 2 5 】

本発明に係る通信端末において、前記受信手段により前記アプリケーションが受信された後に、当該アプリケーションの送信元との通信が切断された場合に、所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段を更に備えるものとしてもよい。

#### 【 0 0 2 6 】

本発明によれば、アプリケーションは、通信端末と送信元との通信が切断された場合に、通信切断時から所定時間が経過したことを契機として削除される。すなわち、通信端末のユーザからの指示を待たずに、アプリケーションの送信元（例えば、アプリケーション配信サーバ）と通信端末との通信が切断された時点から所定時間経過後にアプリケーションは削除される。これにより、アプリケーションが使用される環境から通信端末のユーザが離れたことに伴って、該アプリケーションが削除されることになり、適当でない電子商取引にアプリケーションが使用されることを確実に防止できる。したがって、電子商取引に混乱が生じることがない。その結果、電子購買支援の信頼性が維持される。

#### 【 0 0 2 7 】

本発明に係る価値実体提供サーバにおいて、前記提供手段は、価値実体の提供に先立って、当該価値実体とは別に前記公開鍵を前記通信端末に送信するものとしてもよい。

本発明によれば、価値実体は、公開鍵の送信とは別に価値実体提供サーバから通信端末に提供される。したがって、価値実体提供サーバが価値実体を通信端末に補充する際に、価値実体に公開鍵を添付する必要がないので、価値実体提供サーバと通信端末との間における通信負荷の低減を図ることができる。

#### 【 0 0 2 8 】

本発明に係る価値実体提供サーバにおいて、前記公開鍵は、セルラーネットワークを経由して複数の端末からアクセス可能なサーバ上に公開されているものとしてもよい。

本発明によれば、公開鍵は、価値実体とは独立して、サーバ（例えば価値実体提供サーバ）上に公開されている。これにより、通信端末は、価値実体を使用する際にのみ、サーバにアクセスして公開鍵を取得することが可能となる。したがって、通信端末は、常に公開鍵を保持する必要がなくなり、記憶容量を節約できる。

#### 【 0 0 2 9 】

本発明に係る価値実体提供サーバにおいて、前記提供手段により前記価値実体が提供される前に、前記通信端末のインテグリティを検証する第2検証手段を更に備えるものとしてもよい。本発明によれば、価値実体提供サーバから通信端末に価値実体が提供される前に、通信端末が想定された通りに正常に動作するか否かを示す指標であるインテグリティ（言わば通信端末の信頼性）が検証される。したがって、信頼性の低い通信端末が価値実体を取得することに起因して生じ得る、通信端末のユーザや価値実体の提供元の危害が回避される。

#### 【 0 0 3 0 】

本発明に係るアプリケーション配信サーバは、前記価値実体取得手段により前記価値実体が取得された場合に、当該価値実体が受領された旨が電子的に表現された領収書データを、前記アドホックネットワークを経由して前記通信端末に送信する領収書送信手段を更に備えるものとしてもよい。

**【 0 0 3 1 】**

本発明によれば、アプリケーション配信サーバが価値実体を受領した旨が電子的に表現された領収書データが、アドホックネットワークを経由して、アプリケーション配信サーバから通信端末に送信される。したがって、通信端末が受信した領収書データをユーザが提示することで、アプリケーション配信サーバは、価値実体の送信元が上記通信端末であることを容易に確認することができる。これにより、異なる通信端末（価値実体を送信していない通信端末）のユーザに対して、価値実体の対価としての商品や役務が誤って提供されることをより確実に防止することが可能となる。

**【 0 0 3 2 】**

本発明に係るアプリケーション配信サーバは、前記送信手段により前記アプリケーションが送信される前に、前記通信端末のインテグリティを検証する第3検証手段を更に備えるものとしてもよい。本発明によれば、アプリケーション配信サーバから通信端末にアプリケーションが提供される前に、通信端末が想定された通りに正常に動作するか否かを示す指標であるインテグリティが検証される。したがって、信頼性の低い通信端末がアプリケーションを取得することに起因して、通信端末のユーザやアプリケーションの送信元が危害を被ることが未然に回避される。

**【 0 0 3 3 】****【発明の実施の形態】****（第1の実施の形態）**

以下、添付図面を参照して本発明の第1の実施の形態に係る電子購買支援システムについて説明する。まず、構成を説明する。図1は、本実施の形態における電子購買支援システム1の全体構成の一例を示す模式図である。図1に示すように、電子購買支援システム1は、価値提供サーバ10（価値実体提供サーバに対応）と、携帯端末20（通信端末に対応）と、店舗サーバ30（アプリケーション配信サーバに対応）とを備えて構成されている。

**【 0 0 3 4 】**

更に、価値提供サーバ10と携帯端末20との間には、セルラーネットワーク

N1が形成され、携帯端末20は、基地局B及びセルラーネットワークN1を経由して価値提供サーバ10との間で、相互に各種データの送受信が可能である。セルラーネットワークN1は、通信事業者の管理下にあり、利用者間の通信に際しては、必要に応じて通信相手の認証が行われる。このため、セルラーネットワークN1を経由する通信に関しては、第三者が不正に介入する危険性が低く、比較的安全なデータ送受信を実現可能である。

#### 【0035】

また、携帯端末20と店舗サーバ30の間には、アドホックネットワークN2が形成され、携帯端末20は、アドホックネットワークN2を経由して店舗サーバ30との間で、相互に各種データの無線通信が可能である。アドホックネットワークN2は、特定のインフラストラクチャに依存せず、携帯端末間で一時的に形成されるネットワークである。本実施の形態では、アドホックネットワークN2は、IEEE802.11bやBluetooth等の近距離無線通信規格に準拠した通信網として説明するが、これに限らず、例えばIrDA (Infrared Data Association)、ISO15693、ISO14443等の近傍無線通信規格に準拠した通信網であってもよい。更には、有線通信網であってもよい。

#### 【0036】

アドホックネットワークN2には、拠点となる端末から送信される電波の到達距離に応じて、通信エリアが限定されるという特性がある。したがって、通信相手の位置を特定することが容易であり、携帯端末のロケーションに適応した電子購買支援用のアプリケーションプログラムを配信するのに適している。また、アドホックネットワークN2は、セルラーネットワークN1と比較して高速かつ安価な通信を実現できるので、アプリケーションの様な容量の大きなデータの配信に適している。反面、通信事業者の管理下にないので、悪意や瑕疵のあるアプリケーションが流通する可能性も否定できない。

#### 【0037】

価値提供サーバ10は、ペイメントサービスプロバイダにより運用され、電子購買（電子的に表現された価値実体を用いて商品や役務を売買すること）に際して使用可能な価値実体の発行及び管理（有償無償提供を含む）を行うサーバ装置



である。価値提供サーバ10は、セルラーネットワークN1を経由して、携帯端末20に価値実体を提供する。なお、価値提供サーバ10は、インターネット等の外部ネットワーク上に存在してもよい。この場合、携帯端末20は、通信事業者が運営するゲートウェイを介して、セルラーネットワークN1経由で価値提供サーバ10にアクセスできる。この際、通信安全性を確保する観点から、SSL (Secure Socket Layer) 等の所定のセキュアプロトコルを利用して暗号通信を行ってもよい。

#### 【0038】

携帯端末20は、複数の通信チャネルに対応しており、本実施の形態では、少なくともセルラーネットワークN1及びアドホックネットワークN2を経由した通信が可能である。携帯端末20は、価値提供サーバ10から価値実体を取得する。携帯端末20は、店舗サーバ30から電子購買用のアプリケーションを取得すると共に、該アプリケーションを使用して、上記価値実体を対価とした所望の商品又は役務の購入を支援する。また、携帯端末20は、耐タンパー性を有するデータ格納領域（メモリ）及び暗号演算処理能力を備える。

#### 【0039】

店舗サーバ30は、電子購買が実際に行われる店舗により運用され、電子購買用のアプリケーションを携帯端末20に提供する。店舗サーバ30は、電子購買の利用に供される価値実体を商品又は役務の対価として携帯端末20から取得する。

#### 【0040】

図2は、本実施の形態における電子購買支援システム1の機能的構成を示すシステム構成図である。図2に示すように、価値提供サーバ10は、機能的には、価値実体格納部11と価値実体送信部12（提供手段に対応）とを有する。価値実体格納部11には、アプリケーションの検証に使用される公開鍵A1が添付された価値実体11aが格納されている。価値実体送信部12は、携帯端末20からの要求に応じて、公開鍵A1が添付された価値実体11aを価値実体格納部11から読み出し、セルラーネットワークN1及び基地局Bを介して、携帯端末20宛に該価値実体を送信する。

**【 0 0 4 1 】**

図 2 に示すように、携帯端末 2 0 は、機能的には、価値実体受信部 2 1（取得手段に対応）と、価値実体格納部 2 2 と、アプリケーション受信部 2 3（受信手段に対応）と、アプリケーション検証部 2 4（検証手段に対応）と、アプリケーション起動部 2 5（起動手段に対応）と、アプリケーション削除部 2 6（削除手段に対応）と、価値実体送信部 2 7（移転手段に対応）と、領収書受信部 2 8 とを有する。

**【 0 0 4 2 】**

価値実体受信部 2 1 は、価値提供サーバ 1 0 から送信された価値実体 1 1 a を受信し、公開鍵 A 1 と共に、価値実体格納部 2 2 に格納する。

価値実体格納部 2 2 には、価値実体受信部 2 1 により受信された価値実体 1 1 a が格納される。価値実体格納部 2 2 は、価値実体の秘匿性やシステムの信頼性を確保する観点から、耐タンパー性を有することが好適である。耐タンパー性を実現する手段に関しては、周知慣用の技術であるので詳細な説明は省略するが、特別な材質によりデバイスを構成する、ダミー配線を適宜織り交ぜるといった方法が考えられる（記述の非特許文献 1 参照）。価値実体格納部 2 2 は、例えば、U I M（User Identity Module）や S I M（Subscriber Identity Module）などにより構成される。

アプリケーション受信部 2 3 は、店舗サーバ 3 0 から送信され、電子署名が施されたアプリケーションを受信する。

**【 0 0 4 3 】**

アプリケーション検証部 2 4 は、悪意や瑕疵のあるアプリケーションにより価値実体が不正に使用されることを防ぐために、アプリケーション受信部 2 3 により受信されたアプリケーションが正当性を保証されたものであるか否かの検証を行う。検証は、受信されたアプリケーションに施された電子署名が、価値実体格納部 2 2 内の価値実体 1 1 a に添付されている公開鍵 A 1 に対応しているか否かに基づいて行われる。具体的には、電子署名は秘密鍵 A 2 により暗号化されているので、電子署名されたアプリケーションは秘密鍵 A 2 に対応する公開鍵 A 1 によってしか復号できない。したがって、公開鍵 A 1 が秘密鍵 A 2 に対応するもの

でない場合には、携帯端末 2 0 は、上記アプリケーションを実行することはできないこととなる。

#### 【 0 0 4 4 】

更に、アプリケーション検証部 2 4 は、正当性を保証されたものと判定された（検証に成功した）アプリケーションに対するアクセスを許可すると共に、正当性を保証されていないものと判定された（検証に失敗した）アプリケーションに対するアクセスを拒否する。

#### 【 0 0 4 5 】

アプリケーション起動部 2 5 は、アプリケーション検証部 2 4 による検証の結果、検証に成功したアプリケーションを起動する。

アプリケーション削除部 2 6 は、アプリケーション検証部 2 4 による検証の結果、検証に失敗したアプリケーションを削除する。

#### 【 0 0 4 6 】

価値実体送信部 2 7 は、アプリケーションの検証に成功し、かつ、携帯端末 2 0 のユーザにより商品又は役務の購入が指示された場合に、その対価に相当する額の価値実体を店舗サーバ 3 0 に送信する。

領収書受信部 2 8 は、店舗サーバ 3 0 から送信される、価値実体を受領した旨を示す領収書データを受信する。

#### 【 0 0 4 7 】

図 2 に示すように、店舗サーバ 3 0 は、機能的には、アプリケーション格納部 3 1 と、アプリケーション送信部 3 2 （アプリケーション送信手段に対応）と、価値実体受信部 3 3 （価値実体取得手段に対応）と、領収書送信部 3 4 （領収書送信手段に対応）とを有する。

#### 【 0 0 4 8 】

アプリケーション格納部 3 1 には、店舗サーバ 3 0 が設置されている店舗における電子購買を可能とするためのアプリケーション 3 1 a が格納されている。このアプリケーション 3 1 a は、その提供元によって予め電子署名が施されており、無償又は有償で提供される。アプリケーション 3 1 a は、価値提供サーバ 1 0 の運用元であるペイメントサービスプロバイダが所持又は管理する秘密鍵 A 2 に

より電子署名されている。電子署名は、アプリケーションの提供元を証明すると共に、アプリケーションの正当性を保証するものであり、この電子署名が付されることにより、アプリケーション 31a は、秘密鍵 A2 に対応する公開鍵 A1 が添付された価値実体の使用が可能となる。

#### 【0049】

アプリケーション送信部 32 は、携帯端末 20 からの要求に応じて、アプリケーション 31a をアプリケーション格納部 31 から読み出し、アドホックネットワーク N2 を経由して、携帯端末 20 宛にアプリケーション 31a を送信する。

価値実体受信部 33 は、携帯端末 20 の価値実体送信部 27 により送信された価値実体をアドホックネットワーク N2 を介して受信する。

領収書送信部 34 は、提供された商品又は役務の対価に相当する額の価値実体が受信されたことに伴い、その旨を示す領収書データを携帯端末 20 宛に作成及び送信する。

#### 【0050】

携帯端末 20 は、本発明に係る電子購買支援システムの主要部を構成する端末装置であるので、以下、そのハードウェア構成について詳細に説明する。図 3 は、携帯端末 20 のハードウェア構成図である。携帯端末 20 は、制御装置 20a、入力装置 20b、RAM 20c、表示装置 20d、記憶装置 20e、アンテナ A を伸縮可能に有するセルラーネットワーク通信装置 20f、音声処理装置 20g、及びアドホックネットワーク通信装置 20h を備えて構成される。これら各装置は、それぞれバス 20j によって電氣的に接続されており、相互に信号の入出力が可能となっている。

#### 【0051】

制御装置 20a は、記憶装置 20e に記憶されている電子購買支援プログラムを RAM 20c に読み出し、当該プログラムに従って各部を集中制御する。すなわち、制御装置 20a は、入力装置 20b からの入力信号と RAM 20c に読み出されたプログラムとに従って、後述の電子購買処理を始めとする各種処理を実行し、その処理結果を RAM 20c に一時的に記憶する。そして、RAM 20c に記憶された処理結果を必要に応じて記憶装置 20e 内部の所定領域に格納させ

る。

#### 【 0 0 5 2 】

入力装置 2 0 b は、価値実体及びアプリケーションの送信要求、商品又は役務の選択及び購入等を指示する各種操作ボタンを備えて構成され、これら各種操作ボタンは、単独で又は組み合わせて押下されることにより、指示内容に応じた入力信号を制御装置 2 0 a に出力する。

#### 【 0 0 5 3 】

R A M (Random Access Memory) 2 0 c は、揮発性の半導体メモリにより構成され、制御装置 2 0 a により実行される各種処理において、後述する記憶装置 2 0 e から読み出されたプログラムやデータを一時的に格納する。また、R A M 2 0 c は、表示装置 2 0 d に表示されるデータを一時的に記憶する V R A M (Video RAM) の機能も併有する。

#### 【 0 0 5 4 】

表示装置 2 0 d は、L C D (Liquid Crystal Display) や E L (Electro Luminescence) 等により構成され、制御装置 2 0 a から入力される表示信号に従って、商品メニュー等の表示データの表示を行うユーザインタフェースである。

#### 【 0 0 5 5 】

記憶装置 2 0 e は、E E P R O M (Electrically Erasable and Programmable ROM) 等の不揮発性の半導体メモリにより構成され、各種処理の実行に際して必要なデータや各種処理の実行の結果生成されたデータ等を記憶する。また、記憶装置 2 0 e には、上述した価値実体が格納される。

#### 【 0 0 5 6 】

セルラーネットワーク通信装置 2 0 f は、基地局 B との無線通信の制御を行う。詳細には、セルラーネットワーク通信装置 2 0 f は、信号の変調及び復調を行う変復調部（図示せず）と、信号の符号化及び復号化を行う符復号化部（図示せず）とを有する回路であり、アンテナ A を有する。アンテナ A は、携帯端末 2 0 の筐体上部に伸縮可能に設けられ、基地局 B との間で電波の送受信を行う。

#### 【 0 0 5 7 】

音声処理装置 2 0 g は、変換器、増幅器等により構成され、マイク M 及びスピ

ーカ S を備える。音声処理装置 20 g は、通話時に、制御装置 20 a から入力される音声データを変換器でアナログ信号に変換し、増幅器を介してスピーカ S から放音する。また、音声処理装置 20 g は、通話時に、マイク M から入力される音声信号を変換器によりデジタル信号に変換し、制御装置 20 a に出力する。

#### 【0058】

アドホックネットワーク通信装置 20 h は、無線 LAN の標準規格である IEEE 802.11 b あるいは Bluetooth 等の近距離無線通信規格に準拠しており、アドホックネットワーク N2 との間で直接的にデータの送受信を行う。

#### 【0059】

次に、本実施の形態における電子購買支援システム 1 の動作について説明すると共に、併せて、本発明に係る電子購買支援方法を構成する各ステップについて説明する。

#### 【0060】

本実施の形態では、電子購買処理が実行される店舗として、特に、コーヒESHOP のチェーン店を想定するが、本発明は、かかる店舗においてのみ適用されるものではない。本実施形態におけるチェーン店とは、同種の商品又は役務を統一された商号の下で取り扱う店舗であって、同一の本部の管理下で利益を実現する経営組織形態である。また、価値提供サーバ 10 の運用主体であるペイメントサービスプロバイダは、商品又は役務の販売に関する契約を上記本部と結んでいる。なお、該本部が、ペイメントサービスプロバイダを兼ねてもよい。

#### 【0061】

図 4 は、電子購買支援システム 1 によって実行される電子購買処理の流れを示すフローチャートである。以下に示す各ステップは、図 3 に示した記憶装置 20 e に格納されている電子購買支援プログラムが、制御装置 20 a によって実行されることにより実現する。

#### 【0062】

まず、携帯端末 20 のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提

供サーバ 1 0 の価値実体送信部 1 2 により、公開鍵 A 1 が添付された価値実体 1 1 a が、セルラーネットワーク N 1 及び基地局 B 経由で携帯端末 2 0 宛に送信される (S 1) 。かかる送信処理は、既存の電子商取引の技術により実現可能であるが、第三者によるなりすましを防止するために、予め登録されたパスワードによる認証や認証局による電子認証を利用することが望ましい。

#### 【 0 0 6 3 】

ここで、電子商取引にて提供される多種多様なサービスの中から、価値実体 1 1 a を対価として所望の商品を購入する電子購買サービスを明確に識別するために、必要に応じて、該サービスを一意に特定可能な識別子 (以下、「サービス識別子」と記す。) を価値実体 1 1 a に付与しておくことが好ましい。サービス識別子は、他のサービスとの重複を回避すべく、例えば、価値提供サーバ 1 0 の I P アドレスと、価値提供サーバ 1 0 により生成される文字列の内、過去に使用されていない文字列とが組み合わせられたデータである。

#### 【 0 0 6 4 】

サービス識別子は、価値実体 1 1 a を使用可能なアプリケーションによっても保持されている。かかる識別子は、例えば、アプリケーションのファイル名を示す文字列に含まれている、あるいは、アプリケーションに明示的に割り当てられたメタ情報記述領域に記述されている。したがって、携帯端末 2 0 は、アプリケーションを実行する前に、当該アプリケーションにより特定されるサービスが、価値実体 1 1 a を使用するサービスと一致するか否かを検知することができる。

#### 【 0 0 6 5 】

S 2 では、S 1 で送信された価値実体 1 1 a が、携帯端末 2 0 の価値実体受信部 2 1 により受信され、サービス識別子と対応付けて、価値実体格納部 2 2 に格納される。

#### 【 0 0 6 6 】

S 3 では、携帯端末 2 0 は、アドホックネットワーク N 2 を介して店舗サーバ 3 0 に接続される。かかる接続は、例えば、店舗としてのコーヒーショップ内で店舗サーバ 3 0 により形成される無線 L A N の通信エリア内に携帯端末 2 0 が在圏したことに伴い、アドホックネットワーク通信装置 2 0 h により確立される。

通常、無線 LAN の通信エリアは、コーヒーショップの敷地及びその近傍であるので、遅くとも携帯端末 2 0 のユーザが入店した時点で、携帯端末 2 0 と店舗サーバ 3 0 との間でアドホックネットワークを経由した通信が可能な状態になる。

#### 【 0 0 6 7 】

S 4 では、店舗サーバ 3 0 のアプリケーション送信部 3 2 により、秘密鍵 A 2 により電子署名されたアプリケーション 3 1 a が、アドホックネットワーク N 2 経由で携帯端末 2 0 宛に送信される。かかる送信処理は、店舗サーバ 3 0 が、携帯端末 2 0 を含む携帯端末に対してアプリケーションを強制的に送信するプッシュ型送信であってもよいし、携帯端末 2 0 からの能動的な送信要求を待って送信するプル型送信であってもよい。

#### 【 0 0 6 8 】

S 4 で送信されるアプリケーション 3 1 a は、チェーン店における購買支援を目的とするものであり、店舗サーバ 3 0 が設置されるコーヒーショップに特化したマーケティング戦略や独自のサービス品目又は商品種別に応じて、その設計内容は個別に選定される。また、アプリケーション 3 1 a は、適宜更新可能である。これにより、店舗の特性や経時的変化に適応した効果的な購買支援を可能とする。

#### 【 0 0 6 9 】

S 5 では、S 4 で送信されたアプリケーション 3 1 a が、携帯端末 2 0 のアプリケーション受信部 2 3 により受信され、アプリケーション検証部 2 4 により、公開鍵 A 1 及び電子署名を使用した正当性の検証が行われる。

#### 【 0 0 7 0 】

ここで、価値実体格納部 2 2 に複数種の価値実体が格納されている場合には、検証処理の高速化を図る観点から、検証対象となる価値実体を極力限定する処理が有効となるが、当該処理は、携帯端末 2 0 が、上述したサービス識別子をアプリケーションのファイル名等から検知することにより実現可能である。以下、図 5 を参照しながら、複数種の価値実体が格納されている場合に好適なアプリケーション検証処理について説明する。

#### 【 0 0 7 1 】



図5は、相互に異なる公開鍵が添付された複数の価値実体が格納された価値実体格納部22内のデータ格納例を示す図である。図5に示す様に、価値実体格納部22は、価値実体領域221とサービス識別子領域222とを少なくとも備える。価値実体領域221には、価値提供サーバ10から提供された価値実体11aの他に、公開鍵A1とは異なる公開鍵A2, A3, A4がそれぞれ添付された価値実体が格納されている。サービス識別子領域222には、対応する価値実体領域221内の価値実体を使用されるサービスの識別子（例えば、“0001”, “0002”, “0003”, …）が格納されている。

#### 【0072】

図4に戻り、S5において、アプリケーション検証部24は、受信されたアプリケーションにより特定されるサービス識別子と、サービス識別子領域222内のサービス識別子とを照合する。照合の結果、アプリケーションのサービス識別子に一致するサービス識別子が検知されなかった場合には、その時点で、当該アプリケーションの検証に失敗したことになり、後述のS13以降の処理に移行する。

#### 【0073】

一方、上記照合の結果、アプリケーションのサービス識別子に一致するサービス識別子が検知された場合には、アプリケーションが正当性を有する可能性もあるが、同一のサービス識別子を有する複数の価値実体が検知される可能性、あるいは、アプリケーションの電子署名が価値実体の公開鍵に対応していない可能性も依然としてある。

#### 【0074】

そこで、アプリケーション検証部24は、更に、サービス識別子が一致した価値実体に添付された公開鍵を用いて、受信されたアプリケーションの電子署名を検証する。すなわち、アプリケーション検証部24は、上記アプリケーションが、価値実体の提供元であるペイメントサービスプロバイダによって電子署名されたものであるか、及び、改竄されていないかを検証する。かかる検証は、例えば公開鍵暗号方式により実現可能である。なお、アプリケーションの検証処理は、アプリケーションの受信を契機として自動的に実行されるものとしてもよいし、

ユーザによる入力装置 20b からの指示を待って実行されるものとしてもよい。

#### 【0075】

また、価値実体格納部 22 内に一の価値実体しか格納されていない場合には、サービス識別子の照合処理を行わず、電子署名の検証処理のみを行うものとしてもよい。

その結果、アプリケーション 31a のサービス識別子である“0001”を有し、かつ、秘密鍵 A2 に対応する公開鍵 A1 が添付された価値実体、つまり価値実体 11a の検証は成功する。

#### 【0076】

S5 における検証の結果、アプリケーションの電子署名が価値実体の提供元によって為され、かつ、アプリケーションが改竄されていないものであることが確認されると、アプリケーション検証部 24 は、アプリケーションの検証に成功したものと判断し（S6；Yes）、アプリケーション起動部 25 に対して、アプリケーションの起動を指示する。

#### 【0077】

S7 では、S5 で受信されたアプリケーションは、アプリケーション起動部 26 により起動される。起動されたアプリケーション 31a は、S2 で受信及び格納された価値実体 11a に対するアクセスが可能である。アプリケーション 31a の起動に伴い、携帯端末 20 のユーザが購買可能な商品又は役務が掲載されたメニューリストが表示装置 20d に表示され、制御装置 20a は、ユーザによる入力装置 20b からの購買指示を待機する。購買指示には、ユーザが購買を希望する商品又は役務の識別情報の指定はもとより、個数の指定をも含む。

#### 【0078】

例えば、店舗が上述したチェーン店である場合には、図 6 に示すコーヒーショップメニュー 201 が表示装置 20d に表示される。図 6 に示す様に、コーヒーショップメニュー 201 には、複数のコーヒーの種類が商品名として価格と共に記載されている。ユーザは、所望の商品名（ドライカフェラテ）に対応してその左側に位置するチェックボックス 201a に、入力装置 20b によりチェックすることにより、購買対象となるコーヒーを選択する。チェックボックス 201a

には、所望するコーヒーの個数を入力するようにしてもよい。また、購買対象の選択後に、商品名と個数とをユーザが確認するためのメッセージを表示装置 2 0 d に表示させてもよい。

#### 【0 0 7 9】

より具体的には、コーヒーショップメニュー 2 0 1 において、コーヒーショップが独自にプロモートしている“ドライカフェラテ”が、ユーザの目に留まり易い位置（メニューの冒頭部分に近い領域）に“当店のお薦め”として表示されている。このようにして、電子購買支援システム 1 は、上記本部の管理下にあるコーヒーショップ毎に、独自のマーケティング戦略やロケーションに即した電子購買支援を可能とする。特に、全国展開するチェーン店では、ユーザの嗜好や気象条件が地域毎に異なるので、各コーヒーショップ毎に異なる電子購買支援を行うことは、利便性向上や販売促進の観点から効果的である。更に、“本日のコーヒー”に表示される商品名を適宜（例えば毎日）変更することも、ユーザニーズの変化に即応する意味で有効である。

#### 【0 0 8 0】

図 4 に戻り、購買指示が入力されると（S 8）、携帯端末 2 0 の価値実体送信部 2 7 により、購買を指示された商品又は役務の対価に相当する額（上記例では 3 5 0 円）の価値実体が、価値実体格納部 2 2 内の価値実体 1 1 a から差し引かれ、該価値実体が、アドホックネットワーク N 2 経由で店舗サーバ 3 0 宛に送信される（S 9）。かかる送信処理は、例えば、文献（「情報セキュリティ技術」

2000年8月 社団法人電気通信協会発行 伊土誠一監修、松本隆明、岡本龍明編著）に記載されている既存の電子マネー送受信技術により実現可能である。

#### 【0 0 8 1】

なお、商品又は役務の対価に相当する価値実体が価値実体 1 1 a よりも大きい場合には、価値実体送信部 2 7 は、価値実体の減算及び送信を行わずに、残高が不足している旨のメッセージを表示装置 2 0 d に表示させる。また、不足額分の価値実体がポストペイ（後払い）方式により補填されるものとしてもよい。

#### 【0 0 8 2】

S 1 0 では、携帯端末 2 0 から送信された価値実体が、店舗サーバ 3 0 の価値

実体受信部 33 により受信される。

S11では、店舗サーバ30の領収書送信部34により、商品又は役務の対価に相当する価値実体を受信した旨が電子的に表現されたデータ（領収書データ）が、アドホックネットワークN2経由で携帯端末20宛に送信される。

#### 【0083】

S12では、店舗サーバ30から送信された領収書データが、携帯端末20の領収書受信部28により受信される。受信された領収書データは、アプリケーション31aにより、レンダリング可能な形式に変換され表示装置20dに表示される。ここで、領収書の発行元を容易に識別可能とすると共に偽造を防止するために、コーヒーショップが選定した背景色を領収書データに使用したり、所定のアイコン（絵文字）を挿入してもよい。また、領収書の二重使用を予防するために、背景色やアイコンを所定の時間間隔で変更してもよい。更に、領収書データに、発行日時を示すタイムスタンプを入れてもよい。

#### 【0084】

コーヒーショップは、購入者である携帯端末20のユーザに対して、領収書データを表示装置20dに表示させることを求め、該領収書データの正当性を確認した後に、商品（上記例ではドライカフェラテ）を提供する。

#### 【0085】

なお、領収書は端末間で送受信されるとは限らない。すなわち、S10において価値実体を受信されたことに伴い、その旨を知覚した店舗の店員が、該価値実体に相当する対価を受領した旨が表記された物理的な（紙媒体の）領収書を印刷出力し、ユーザに手渡すものとしても勿論よい。

#### 【0086】

S5における検証の結果、アプリケーションの電子署名が価値実体の提供元によって為されていないこと、又は、アプリケーションが改竄されていることが確認されると、アプリケーション検証部24は、アプリケーションの検証に失敗したものと判断し（S6；No）、アプリケーション削除部26に対して、アプリケーションの削除を指示する。

#### 【0087】

S 1 3 では、S 5 で受信されたアプリケーションは、アプリケーション削除部 2 6 により削除される。無線 LAN を始めとするアドホックネットワークでは、通信事業者を介さずに端末装置間で直接的に通信が行われるので、通信内容が傍受されたり、コーヒショップ以外の第三者が無線 LAN による別のサービスを近傍のエリアで提供したりすることが予見される。しかし、アプリケーションを削除することにより、悪意のある第三者により作成、又は改竄された可能性のあるアプリケーションを実行することに伴って生じる様々な危害が未然に防止される。その結果、電子購買支援システム 1 に関して高いセキュリティレベルを確保できる。

#### 【 0 0 8 8 】

S 1 4 では、S 5 で受信されたアプリケーションが削除された旨を示すメッセージが表示装置 2 0 d に表示される。メッセージは、例えば、「取得したアプリケーションの検証に失敗しました。このため、アプリケーションを削除しました。」なるテキストデータである。これにより、携帯端末 2 0 のユーザは、アプリケーションの検証に失敗した旨、及びアプリケーションが削除された旨を容易に認識できる。なお、アプリケーションの削除処理は、ユーザによる入力装置 2 0 b からの指示を待って実行されるものとしてもよい。

#### 【 0 0 8 9 】

以上説明した様に、第 1 の実施形態における電子購買支援システム 1 によれば、店舗サーバ 3 0 から送信されたアプリケーションが必ずしも安全なものではない場合を懸念して、価値提供サーバ 1 0 から事前に取得された価値実体に対する上記アプリケーションのアクセスを許可すべきか否かを検証する。かかる検証を行うための手段として、価値実体に予め添付された公開鍵と、アプリケーションの電子署名に使用された秘密鍵との作成元が一致するか否かを判定する。携帯端末 2 0 は、検証が成功した場合にのみ、アプリケーションによる価値実体へのアクセスを許可し、当該アプリケーションを使用して店舗サーバ 3 0 に価値実体を移転する。

#### 【 0 0 9 0 】

これにより、提供元が保証されていないアプリケーションや改竄されたアプリ

ケーションが価値実体にアクセスすることが未然に防止され、価値実体が不正に使用されることがない。その結果、アドホックネットワークを使用して価値実体のやり取りを行う場合においても、安全かつ容易な電子購買支援が実現される。

#### 【0091】

(第2の実施の形態)

次に、本発明における第2の実施の形態について説明する。

第1の実施形態では、価値実体は、対応する公開鍵と共に、価値提供サーバ10から携帯端末20に送信されるものとしたが、本実施の形態では、価値実体と公開鍵とはそれぞれ個別に送信される。

#### 【0092】

本実施の形態における電子購買支援システムは、第1の実施形態において詳述した電子購買支援システム1と機能的構成を同様とする。また、本実施の形態における携帯端末は、上述した携帯端末20とハードウェア構成を同一とする。したがって、共通する構成要素には同一の符号を付し、その説明は省略すると共に、第1の実施の形態との差異について詳述する。

#### 【0093】

以下、図7を参照して、第2の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第1の実施形態において詳述した電子購買処理(図4参照)と共通するステップを複数含む。具体的には、図7のS25～S36の各ステップは、図4に示したS3～S14の各ステップにそれぞれ相当する。

#### 【0094】

以下、本実施の形態に特有のステップであるS21～S24(図7中の太線で囲んだ処理)について説明する。まず、S21では、携帯端末20のユーザが、ペイメントサービスプロバイダと商品又は役務の売買に関する契約を締結したこと、又は、該プロバイダへのアカウントを作成したことに伴い、価値提供サーバ10の価値実体送信部12により、公開鍵A1が、セルラーネットワークN1及び基地局B経由で携帯端末20宛に送信される。

## 【 0 0 9 5 】

S 2 2 では、S 2 1 で送信された公開鍵 A 1 が、携帯端末 2 0 の価値実体受信部 2 1 により受信され価値実体格納部 2 2 に格納される。なお、公開鍵 A 1 は、携帯端末 2 0 の製造時等に、記憶装置 2 0 e に予め格納しておくものとしてもよい。

## 【 0 0 9 6 】

S 2 3 では、携帯端末 2 0 のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提供サーバ 1 0 の価値実体送信部 1 2 により、公開鍵 A 1 に対応する価値実体 1 1 a が、セルラーネットワーク N 1 及び基地局 B 経由で携帯端末 2 0 宛に送信される。

## 【 0 0 9 7 】

S 2 4 では、S 2 3 で送信された価値実体 1 1 a が、携帯端末 2 0 の価値実体受信部 2 1 により受信され、公開鍵 A 1 及びサービス識別子と対応付けて、価値実体格納部 2 2 に格納される。

その後、S 2 5 以降の処理が実行されるが、S 2 5 ～ S 3 6 の各ステップは、第 1 の実施形態における S 3 ～ S 1 4 （図 4 参照）の各ステップと同一であるので、その説明は省略する。

## 【 0 0 9 8 】

第 2 の実施形態における電子購買支援システムによれば、S 2 3 及び S 2 4 の処理を繰り返し実行することにより、携帯端末 2 0 への価値実体の補充（チャージ）が可能となる。すなわち、携帯端末 2 0 が価値実体を受信した時点で、価値実体格納部 2 2 に価値実体が残存する場合には、該価値実体の額と、受信された価値実体の額とが加算（マージ）される。この際、価値提供サーバ 1 0 は、送信する価値実体に公開鍵を添付する必要がないので、電子購買処理に伴う通信データ量を低減することができる。

## 【 0 0 9 9 】

（第 3 の実施の形態）

次に、本発明における第 3 の実施の形態について説明する。

第 1 及び第 2 の実施形態では、携帯端末 2 0 は、価値提供サーバ 1 0 から予め取得した公開鍵を、対応する価値実体と共に価値実体格納部 2 2 に格納し、常時保持するものとした。これに対して、本実施の形態では、携帯端末 2 0 は、アプリケーションを使用して電子購買を行う都度、価値提供サーバ 1 0 に公開鍵の送信を要求して取得する。

#### 【 0 1 0 0 】

図 8 は、本実施の形態における電子購買支援システム 2 の機能的構成を示すシステム構成図である。電子購買支援システム 2 は、第 1 及び第 2 の実施形態における電子購買支援システム 1 と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末 2 0 とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、上記各実施の形態との差異について詳述する。

#### 【 0 1 0 1 】

図 8 に示すように、価値提供サーバ 1 0 は、機能的には、価値実体格納部 1 1 と公開鍵公開部 1 3 と価値実体送信部 1 2 と公開鍵送信部 1 4 とを有する。

価値実体格納部 1 1 には、店舗における商品又は役務の電子購買に使用される価値実体 1 1 b が格納されている。

公開鍵公開部 1 3 は、アプリケーション 3 1 a の起動に必要な公開鍵 A 1 を更新可能に保持する。公開鍵公開部 1 3 は、携帯端末 2 0 を含む複数の携帯端末がセルラーネットワーク N 1 を経由してアクセス可能な形態で公開鍵 A 1 を公開する。

#### 【 0 1 0 2 】

価値実体送信部 1 2 は、携帯端末 2 0 からの価値実体送信要求に応じて、価値実体 1 1 b を価値実体格納部 1 1 から読み出し、セルラーネットワーク N 1 及び基地局 B を介して携帯端末 2 0 宛に送信する。

公開鍵送信部 1 4 は、携帯端末 2 0 からの公開鍵送信要求に応じて、公開鍵 A 1 を公開鍵公開部 1 3 から取得し、セルラーネットワーク N 1 及び基地局 B を介して携帯端末 2 0 宛に送信する。

#### 【 0 1 0 3 】



図 8 に示すように、携帯端末 20 は、機能的には、価値実体受信部 21 と、価値実体格納部 22 と、アプリケーション受信部 23 と、公開鍵送信要求部 29 と、公開鍵受信部 210 と、アプリケーション検証部 24 と、アプリケーション起動部 25 と、アプリケーション削除部 26 と、価値実体送信部 27 と、領収書受信部 28 とを有する。

#### 【0104】

公開鍵送信要求部 29 は、アプリケーション受信部 23 によるアプリケーション 31a の受信に伴って、アプリケーション 31a の起動に必要な公開鍵（公開鍵 A1）の送信を、価値提供サーバ 10 に対して要求する。

公開鍵受信部 210 は、価値提供サーバ 10 の公開鍵送信部 14 により送信された公開鍵 A1 を受信し、公開鍵 A1 を使用してアプリケーション 31a を検証することをアプリケーション検証部 24 に指示する。

#### 【0105】

以下、図 9 を参照して、第 3 の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第 1 の実施形態において詳述した電子購買処理（図 4 参照）と共通するステップを複数含む。具体的には、図 9 の S44, S45, S49～S57 の各ステップは、図 4 に示した S3, S4, S6～S14 の各ステップにそれぞれ相当する。

#### 【0106】

以下、本実施の形態に特有のステップである S41～S43, S46, S47（図 9 中の太線で囲んだ処理）について説明する。まず、S41 では、価値提供サーバ 10 の公開鍵公開部 13 により、公開鍵 A1 が、携帯端末 20 からセルラーネットワーク N1 を経由してアクセスが可能な形態で公開される。

#### 【0107】

S42 では、携帯端末 20 のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提供サーバ 10 の価値実体送信部 12 により、公開鍵 A1 に対応する価値実体 11a が、セルラーネットワーク N1 及び基地局 B 経由で携帯端末 20 宛に送

信される。

【0 1 0 8】

S 4 3 では、S 4 2 で送信された価値実体 1 1 a が、携帯端末 2 0 の価値実体受信部 2 1 により受信され、サービス識別子と対応付けて、価値実体格納部 2 2 に格納される。この時点では、公開鍵 A 1 は、携帯端末 2 0 に存在しない。

【0 1 0 9】

携帯端末 2 0 が、アドホックネットワーク N 2 により店舗サーバ 3 0 に接続されると (S 4 4)、店舗サーバ 3 0 からアドホックネットワーク N 2 を経由して携帯端末 2 0 宛にアプリケーション 3 1 a が送信される (S 4 5)。

S 4 6 では、アプリケーション 3 1 a の受信を契機として、公開鍵送信要求部 2 9 により、アプリケーション 3 1 a の起動に必要な公開鍵 A 1 の送信要求が、価値提供サーバ 1 0 宛に送信される。この送信要求は、秘匿性及び安全性の高いセルラーネットワーク N 1 を経由して送信される。

【0 1 1 0】

S 4 7 では、S 4 6 で送信された公開鍵送信要求に応じて、公開鍵送信部 1 4 により、公開鍵公開部 1 3 から公開鍵 A 1 が取得され、セルラーネットワーク N 1 経由で携帯端末 2 0 宛に送信される。

【0 1 1 1】

S 4 7 で送信された公開鍵 A 1 は、携帯端末 2 0 の公開鍵受信部 2 1 0 により受信される (S 4 8)。公開鍵 A 1 の受信に伴い、携帯端末 2 0 は、アプリケーション検証部 2 4 により、S 4 6 で受信されたアプリケーション 3 1 a の検証を開始する。その後、S 4 9 以降の処理が実行されるが、S 4 9 ~ S 5 7 の各ステップは、第 1 の実施形態における S 6 ~ S 1 4 (図 4 参照) の各ステップと同一であるので、その説明は省略する。

【0 1 1 2】

第 3 の実施形態における電子購買支援システム 2 によれば、ペイメントサービスプロバイダが価値提供サーバ 1 0 上に公開鍵 A 1 を公開しておくことにより、携帯端末 2 0 は、公開鍵 A 1 を常時保持していなくとも、必要に応じて、価値提供サーバ 1 0 から公開鍵 A 1 を取得することができる。したがって、携帯端末 2

0 のデータ記憶容量を節約できる。

#### 【0 1 1 3】

また、秘密鍵 A 2 を適宜更新することは、電子購買支援の安全性向上に資するが、秘密鍵 A 2 の更新に遅滞なく、携帯端末 2 0 の保持する公開鍵 A 1 を更新することは困難である。そこで、電子購買支援システム 2 では、携帯端末 2 0 が、アプリケーション 3 1 a を受信する度に公開鍵 A 1 を能動的に取得する。これにより、携帯端末 2 0 のユーザは、秘密鍵 A 2 が更新された場合でも、最新の秘密鍵 A 2 に対応する公開鍵 A 1 を確実かつ容易に入手することができる。その結果、電子購買支援システム 2 は、高いセキュリティを維持しつつ、容易な電子購買を提供できる。

#### 【0 1 1 4】

(第 4 の実施の形態)

次に、本発明における第 4 の実施の形態について説明する。

第 1 ～第 3 の実施形態では、携帯端末 2 0 は、受信したアプリケーションの検証に失敗した時に、該アプリケーションを削除するものとした。これに対して、本実施の形態では、携帯端末 2 0 は、アプリケーションを受信した時点から所定時間が経過したことを契機として自動的にアプリケーションを削除する。以下、第 1 の実施形態における電子購買支援システム 1 に経過時間測定機能を付加した電子購買支援システム 3 について代表的に説明するが、第 2 及び第 3 の実施形態における電子購買支援システムに関しても本機能を適用することは可能である。

#### 【0 1 1 5】

図 1 0 は、本実施の形態における電子購買支援システム 3 の機能的構成を示すシステム構成図である。電子購買支援システム 3 は、第 1 の実施形態における電子購買支援システム 1 と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末 2 0 とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、第 1 の実施形態との差異について詳述する。

#### 【0 1 1 6】

店舗サーバ 3 0 から携帯端末 2 0 に送信されるアプリケーション 3 1 a には、

店舗によって任意に設定された所定時間 T1（例えば 1～3 時間程度）が予め記述されている。

図 10 に示すように、携帯端末 20 は、機能的には、価値実体受信部 21 と、価値実体格納部 22 と、アプリケーション受信部 23 と、経過時間測定部 211 と、アプリケーション検証部 24 と、アプリケーション起動部 25 と、アプリケーション削除部 26 と、価値実体送信部 27 と、領収書受信部 28 とを有する。

#### 【0117】

経過時間測定部 211 は、アプリケーション受信部 23 によりアプリケーション 31a が受信された時点で、経過時間の測定を開始する。同時に、経過時間測定部 211 は、アプリケーション 31a から所定時間 T1 を取得し、上記経過時間が所定時間 T1 に到達するのを待機する。経過時間測定部 211 は、上記経過時間が所定時間 T1 に到達したことを契機として、アプリケーション削除部 26 に対し、アプリケーション 31a の削除を指示する。

#### 【0118】

アプリケーション削除部 26 は、経過時間測定部 211 からの指示に応じて、アプリケーション 31a を削除する。なお、アプリケーション 31a により作成されたファイルがあれば、アプリケーション削除部 26 は、これも削除する。該ファイルとは、例えば、レンダリング可能な形式に変換された領収書データである。

#### 【0119】

第 4 の実施形態における電子購買支援システム 3 によれば、アプリケーション 31a は、携帯端末 20 により受信された時点からの所定時間の経過に伴い、自動的に削除される。これにより、アプリケーション 31a は、携帯端末 20 内に所定時間を超えて留まることがない。したがって、アプリケーション 31a 又はこれにより作成されたファイルが、別の店舗で使用され、電子商取引に混乱が生じる恐れを回避できる。

#### 【0120】

更に、第 4 の実施形態の変形態様として、携帯端末 20 は、アプリケーション 31a を受信した後も店舗サーバ 30 との間に通信セッションを継続すると共に

、経過時間測定部 2 1 1 は、該通信セッションが切断された時点で、経過時間の測定を開始するものとしてもよい。この場合においても、経過時間測定部 2 1 1 は、計時開始と同時に、アプリケーション 3 1 a から所定時間 T 2（例えば 5 分程度）を取得し、上記経過時間が所定時間 T 2 に到達するのを待機する。経過時間測定部 2 1 1 は、上記経過時間が所定時間 T 2 に到達したことを契機として、アプリケーション削除部 2 6 に対し、アプリケーション 3 1 a の削除を指示する。

#### 【0 1 2 1】

アプリケーション削除部 2 6 は、経過時間測定部 2 1 1 からの指示に応じて、アプリケーション 3 1 a を削除する。なお、アプリケーション 3 1 a により作成されたファイルがあれば、アプリケーション削除部 2 6 はこれも削除する。該ファイルとは、例えば、レンダリング可能な形式に変換された領収書データである。

#### 【0 1 2 2】

通信セッションの切断は、アドホックネットワーク N 2 の通信圏内から携帯端末 2 0 が離れる等の外的要因により生じる。本変形態様における電子購買支援システムによれば、アプリケーション 3 1 a は、通信セッションの切断を契機として削除される。換言すれば、アプリケーション 3 1 a が保持される時間は、通信セッションの継続時間に依存することになり、携帯端末 2 0 のユーザが店舗から退出したことに起因して、アプリケーション 3 1 a は、迅速かつ確実に携帯端末 2 0 から削除される。したがって、アプリケーション 3 1 a が別の店舗で使用され、電子商取引に混乱が生じる懸念を解消できる。

#### 【0 1 2 3】

また、通信環境によっては、アプリケーション 3 1 a の受信完了後かつ検証完了前に何らかの要因により通信が切断され、検証処理を経していないアプリケーション 3 1 a が携帯端末 2 0 に残る可能性がある。そこで、かかる場合には、アプリケーション削除部 2 6 は、所定時間の経過を待ってアプリケーション 3 1 a を自動的に削除することにより、正当性が保証されていないアプリケーションが携帯端末 2 0 に保持されることを未然に防止できる。所定時間は、アプリケーショ

ン 31a の受信直後に当該アプリケーションが価値実体の移転に使用される事態を回避する観点から、十分に短い時間（例えば 1 ～ 3 秒程度）であることが望ましい。

#### 【0124】

（第 5 の実施の形態）

次に、本発明における第 5 の実施の形態について説明する。

本実施の形態では、携帯端末は、想定された通りに正常に動作するか否かを示す指標であるインテグリティを測定する機能を有する。価値提供サーバは、携帯端末から送信された測定結果を検証し、検証に成功した場合にのみ、携帯端末宛に価値実体を送信する。同様に、店舗サーバは、上記測定結果の検証に成功した場合にのみ、携帯端末宛にアプリケーションを送信する。

#### 【0125】

以下、第 1 の実施形態における電子購買支援システム 1 の携帯端末 20 にインテグリティ測定機能を付加した電子購買支援システム 4 について代表的に説明するが、第 2 ～ 第 4 の実施形態における電子購買支援システムに関しても本機能を適用することは可能である。

#### 【0126】

図 11 は、本実施の形態における電子購買支援システム 4 の機能的構成を示すシステム構成図である。電子購買支援システム 4 は、第 1 の実施形態における電子購買支援システム 1 と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末 20 とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、第 1 の実施形態との差異について詳述する。

#### 【0127】

図 11 に示すように、価値提供サーバ 10 は、機能的には、価値実体格納部 11 と、測定結果送信要求部 15 と、測定結果受信部 16 と、測定結果検証部 17（第 2 検証手段に対応）と、価値実体送信部 12 とを有する。測定結果送信要求部 15 は、携帯端末 20 に対して、インテグリティの測定結果の送信を要求する。測定結果受信部 16 は、携帯端末 20 の測定結果送信部 213 により送信され

た上記測定結果をセルラーネットワークN1経由で受信する。

【0128】

測定結果検証部17は、測定結果受信部16により受信された上記測定結果を検証し、携帯端末20における信頼性の有無を判定する。インテグリティ測定結果の検証処理に関しては、例えば、文献(Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel Corporation, Microsoft Corporation,「Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b」, 22 February 2002, [http://www.trustedcomputing.org/docs/main%20v1\\_1b.pdf](http://www.trustedcomputing.org/docs/main%20v1_1b.pdf))に記載されている既存の技術により実現可能である。

【0129】

携帯端末20は、機能的には、インテグリティ測定部212と、測定結果送信部213と、価値実体受信部21と、価値実体格納部22と、アプリケーション受信部23と、アプリケーション検証部24と、アプリケーション起動部25と、アプリケーション削除部26と、価値実体送信部27と、領収書受信部28とを有する。

【0130】

インテグリティ測定部212は、既存技術であるTPM (Trusted Platform Module) が携帯端末20の制御装置20aにより実行されることにより実現する機能を有し、携帯端末20のインテグリティを測定する。インテグリティの測定処理に関しても、例えば、上記文献に記載の技術により実現可能である。

【0131】

測定結果送信部213は、インテグリティ測定部212によるインテグリティ測定結果を価値提供サーバ10宛に送信する。

【0132】

店舗サーバ30は、機能的には、アプリケーション格納部31と、測定結果送信要求部35と、測定結果受信部36と、測定結果検証部37 (第3検証手段に対応) と、アプリケーション送信部32と、価値実体受信部33と、領収書送信部34とを有する。測定結果送信要求部35は、携帯端末20に対して、インテグリティの測定結果の送信を要求する。測定結果受信部36は、携帯端末20の

測定結果送信部 213 により送信された上記測定結果をアドホックネットワーク N2 経由で受信する。測定結果検証部 37 は、測定結果受信部 36 により受信された上記測定結果を検証し、携帯端末 20 における信頼性の有無を判定する。

#### 【0133】

以下、図 12 を参照して、第 5 の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第 1 の実施形態において詳述した電子購買処理（図 4 参照）と共通するステップを複数含む。具体的には、図 12 の S66～S68、S74～S76 の各ステップは、図 12 に示した S1～S3、S4～S6 の各ステップにそれぞれ相当する。S76 の後処理に関しては図示しないが、図 4 に示した S7 以降の処理と同一の処理が実行される。

#### 【0134】

以下、本実施の形態に特有のステップである S61～S65、S69～S73（図 12 中の太線で囲んだ処理）について説明する。まず、S61 では、価値提供サーバ 10 の公開鍵公開部 13 により、公開鍵 A1 が、携帯端末 20 からセルラーネットワーク N1 を経由してアクセスが可能な形態で公開される。

#### 【0135】

S61 では、価値提供サーバ 10 が携帯端末 20 の信頼性を確認すべく、価値提供サーバ 10 の測定結果送信要求部 15 により、インテグリティの送信要求が携帯端末 20 宛に送信される。この送信要求は、秘匿性及び安全性の高いセルラーネットワーク N1 を経由して送信される。

#### 【0136】

S62 では、S61 にて送信された送信要求に応じて、インテグリティ測定部 212 により、携帯端末 20 のインテグリティが測定される。

S63 では、S62 にて測定されたインテグリティが、測定結果送信部 213 により、セルラーネットワーク N1 経由で価値提供サーバ 10 宛に送信される。

#### 【0137】

S64 では、S63 にて携帯端末 20 から送信されたインテグリティ測定結果が測定結果受信部 16 により受信され、測定結果検証部 17 により該測定結果が



検証される。検証の結果、インテグリティの検証に成功した場合には（S 6 5 ; Y e s）、S 6 6に進み、公開鍵 A 1 が添付された価値実体 1 1 a が、セルラーネットワーク N 1 及び基地局 B 経由で携帯端末 2 0 宛に送信される。

【0138】

S 6 4 における検証の結果、インテグリティの検証に失敗した場合には（S 6 5 ; N o）、一連の電子購買処理を終了する。インテグリティの検証に失敗する要因としては、例えば、携帯端末 2 0 がウイルスに感染している等の理由により信頼できない状態にある場合が挙げられる。

【0139】

携帯端末 2 0 と店舗サーバ 3 0 とが接続されると（S 6 8）、S 6 9では、店舗サーバ 3 0 が携帯端末 2 0 の信頼性を確認すべく、店舗サーバ 3 0 の測定結果送信要求部 3 5 により、インテグリティの送信要求が携帯端末 2 0 宛に送信される。

【0140】

S 7 0 では、S 6 9 にて送信された送信要求に応じて、インテグリティ測定部 2 1 2 により、携帯端末 2 0 のインテグリティが測定される。

S 7 1 では、S 7 0 にて測定されたインテグリティが、測定結果送信部 2 1 3 により、アドホックネットワーク N 2 経由で店舗サーバ 3 0 宛に送信される。

【0141】

S 7 2 では、S 7 1 にて携帯端末 2 0 から送信されたインテグリティ測定結果が測定結果受信部 3 6 により受信され、測定結果検証部 3 7 により当該測定結果が検証される。検証の結果、インテグリティの検証に成功した場合には（S 7 3 ; Y e s）、S 7 4 に進み、アプリケーション格納部 3 1 内のアプリケーション 3 1 a が、アドホックネットワーク N 2 経由で携帯端末 2 0 宛に送信される。一方、インテグリティの検証に失敗した場合には（S 7 3 ; N o）、一連の電子購買処理を終了する。

【0142】

第 5 の実施形態における電子購買支援システム 4 によれば、価値提供サーバ 1 0 は、価値実体を送信する前に、その送信先である携帯端末 2 0 のインテグリテ

ィ測定結果を取得し、この測定結果に基づいて携帯端末 2 0 の信頼性の有無を判定する。そして、信頼性があると判断された携帯端末に対してのみ価値実体を送信する。したがって、ウイルス感染や悪意による改造の可能性のある携帯端末が価値実体を取得することに起因して、電子購買支援システムに危害が及び、信頼性が低下することを未然に防止できる。

#### 【0 1 4 3】

また、第 5 の実施形態における電子購買支援システム 4 によれば、店舗サーバ 3 0 は、アプリケーションを送信する前に、その送信先である携帯端末 2 0 のインテグリティ測定結果を取得し、この測定結果に基づいて携帯端末 2 0 の信頼性の有無を判定する。そして、信頼性があると判断された携帯端末に対してのみアプリケーションを送信する。これにより、携帯端末 2 0 のインテグリティは、価値実体の受信直前に限らず、アプリケーションの受信直前にも再び検証されることになる。したがって、例えば、携帯端末 2 0 が価値実体を受信した時点ではインテグリティに問題はなかったが受信後にインテグリティが低下した場合などに、携帯端末 2 0 が不適切に振る舞って、電子購買支援システムに危害が及び、信頼性が低下することを回避できる。

#### 【0 1 4 4】

最後に、上述した一連の電子購買処理を携帯端末 2 0 に実行させるための電子購買支援プログラムについて説明する。図 1 3 に示すように、電子購買支援プログラム 4 1 は、記録媒体 4 0 に形成されたプログラム格納領域 4 0 a 内に格納されている。

#### 【0 1 4 5】

電子購買支援プログラム 4 1 は、電子購買処理を統括的に制御するメインモジュール 4 1 a と、外部から送信された価値実体を受信する処理を携帯端末 2 0 に実行させる価値実体受信モジュール 4 1 b と、受信された価値実体をメモリ等の格納手段に格納する処理を携帯端末 2 0 に実行させる価値実体格納モジュール 4 1 c と、外部から送信されたアプリケーションを受信する処理を携帯端末 2 0 に実行させるアプリケーション受信モジュール 4 1 d と、受信されたアプリケーションを検証する処理を携帯端末 2 0 に実行させるアプリケーション検証モジュール

ル 4 1 e と、検証に成功したアプリケーションを起動する処理を携帯端末 2 0 に実行させるアプリケーション起動モジュール 4 1 f と、検証に失敗したアプリケーションを削除する処理を携帯端末 2 0 に実行させるアプリケーション削除モジュール 4 1 g と、アプリケーションの送信元宛に価値実体を送信する処理を携帯端末 2 0 に実行させる価値実体送信モジュール 4 1 h と、外部から送信された、価値実体に対する領収書データを受信する処理を携帯端末 2 0 に実行させる領収書受信モジュール 4 1 i とを備えて構成される。

#### 【0146】

価値実体受信モジュール 4 1 b と、アプリケーション受信モジュール 4 1 d と、アプリケーション検証モジュール 4 1 e と、アプリケーション起動モジュール 4 1 f と、アプリケーション削除モジュール 4 1 g と、価値実体送信モジュール 4 1 h と、領収書受信モジュール 4 1 i の各モジュールを実行させることによって実現する機能は、携帯端末 2 0 の有する価値実体受信部 2 1 と、アプリケーション受信部 2 3 と、アプリケーション検証部 2 4 と、アプリケーション起動部 2 5 と、アプリケーション削除部 2 6 と、価値実体送信部 2 7 と、領収書受信部 2 8 の機能と同様である。また、価値実体格納モジュール 4 1 c を実行させることによって格納されるデータは、価値実体格納部 2 2 に格納されるデータと同様である。

#### 【0147】

電子購買支援プログラム 4 1 は、その一部若しくは全部が、通信回線等の伝送媒体を介して伝送され、他の機器により受信されて記録（インストールを含む）される構成としてもよい。

#### 【0148】

##### 【発明の効果】

本発明によれば、アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことが可能となる。

##### 【図面の簡単な説明】

#### 【図 1】

電子購買支援システムの全体構成を概念的に示す図である。

**【図 2】**

第 1 及び第 2 の実施形態における電子購買支援システムの機能的構成を示す図である。

**【図 3】**

携帯端末のハードウェア構成を示すブロック図である。

**【図 4】**

第 1 の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

**【図 5】**

複数種の価値実体が格納されている場合における価値実体格納部のデータ格納例を示す図である。

**【図 6】**

電子購買処理の実行に際して、携帯端末の表示装置に表示される商品メニューの一例を示す図である。

**【図 7】**

第 2 の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

**【図 8】**

第 3 の実施形態における電子購買支援システムの機能的構成を示す図である。

**【図 9】**

第 3 の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

**【図 1 0】**

第 4 の実施形態の変形態様における電子購買支援システムの機能的構成を示す図である。

**【図 1 1】**

第 5 の実施形態における電子購買支援システムの機能的構成を示す図である。

**【図 1 2】**

第 5 の実施形態における電子購買支援システムによって実行される電子購買処

理の流れを示すフローチャートである。

【図 13】

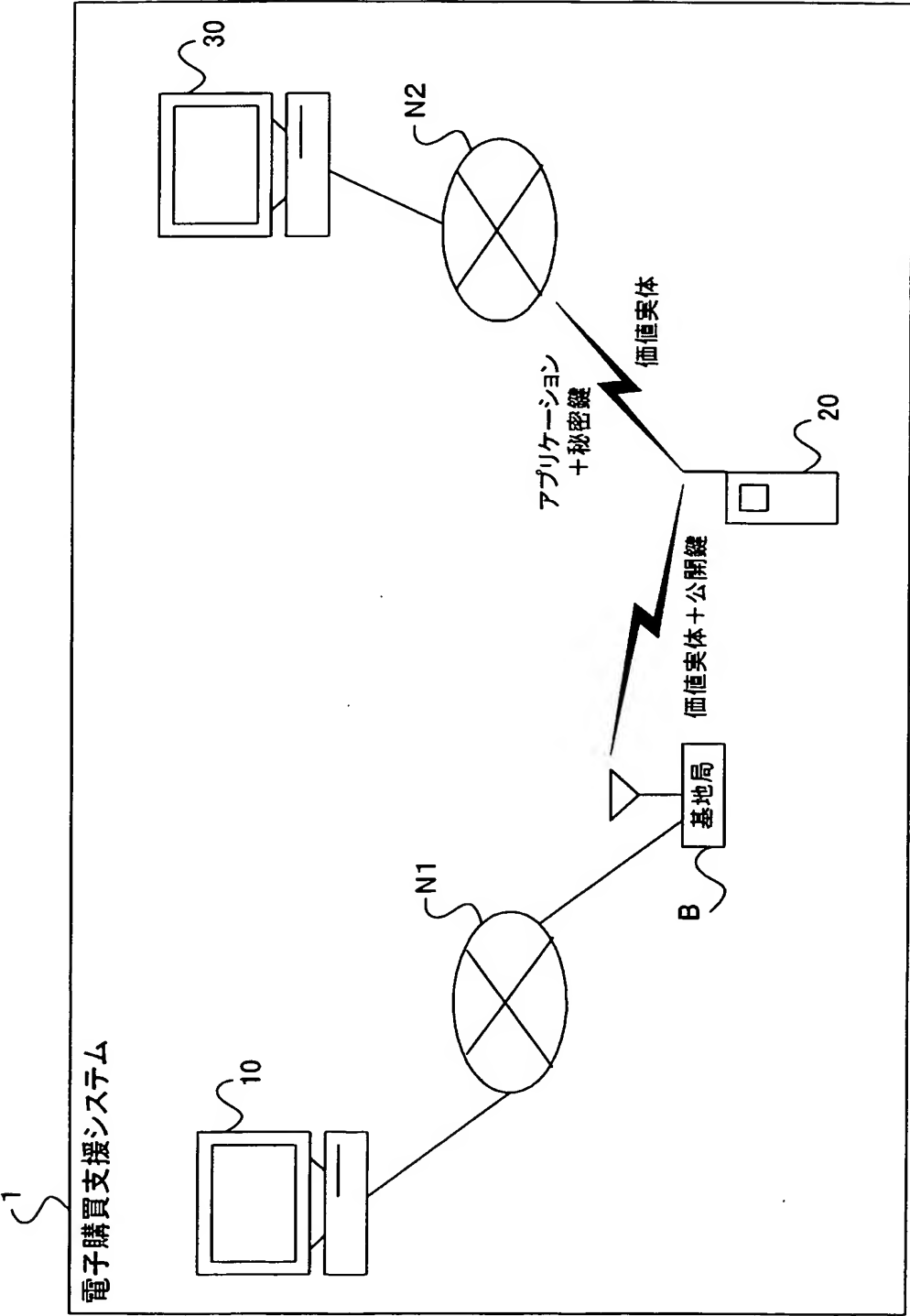
本発明に係る電子購買支援プログラムの構成を示す図である。

【符号の説明】

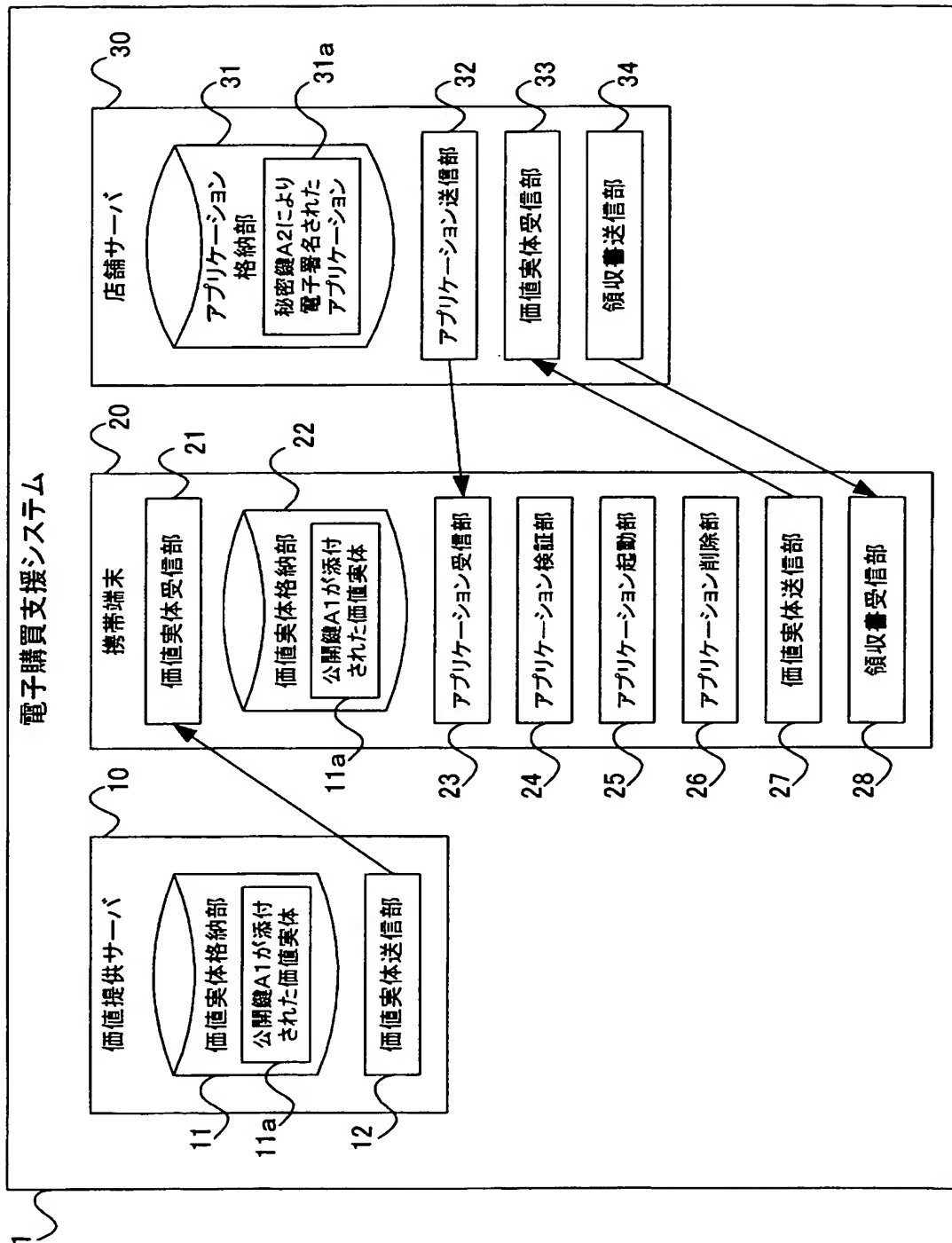
1…電子購買支援システム、10…価値提供サーバ、11…価値実体格納部、  
11a…価値実体、12…価値実体送信部、13…公開鍵公開部、14…公開鍵  
送信部、15…測定結果送信要求部、16…測定結果受信部、17…測定結果検  
証部、212…インテグリティ測定部、213…測定結果送信部、35…測定結  
果送信要求部、36…測定結果受信部、37…測定結果検証部、212…インテ  
グリティ測定部、20…携帯端末、21…価値実体受信部、22…価値実体格納  
部、23…アプリケーション受信部、24…アプリケーション検証部、25…ア  
プリケーション起動部、26…アプリケーション削除部、27…価値実体送信部  
、28…領収書受信部、29…公開鍵送信要求部、210…公開鍵受信部、21  
1…経過時間測定部、30…店舗サーバ、31…アプリケーション格納部、31  
a…アプリケーション、32…アプリケーション送信部、33…価値実体受信部  
、34…領収書送信部、A1…公開鍵、A2…秘密鍵

【書類名】 図面

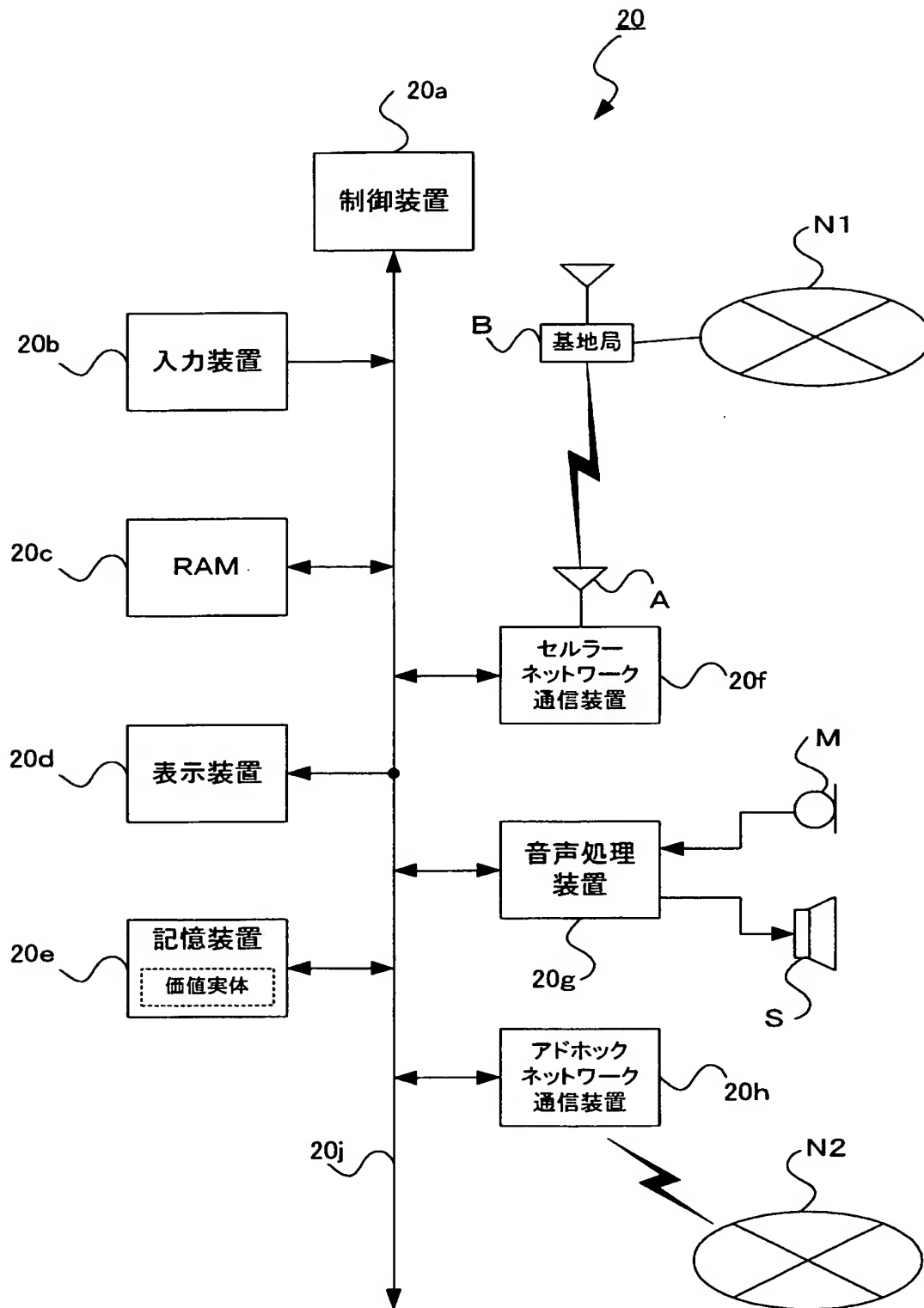
【図 1】



【図 2】

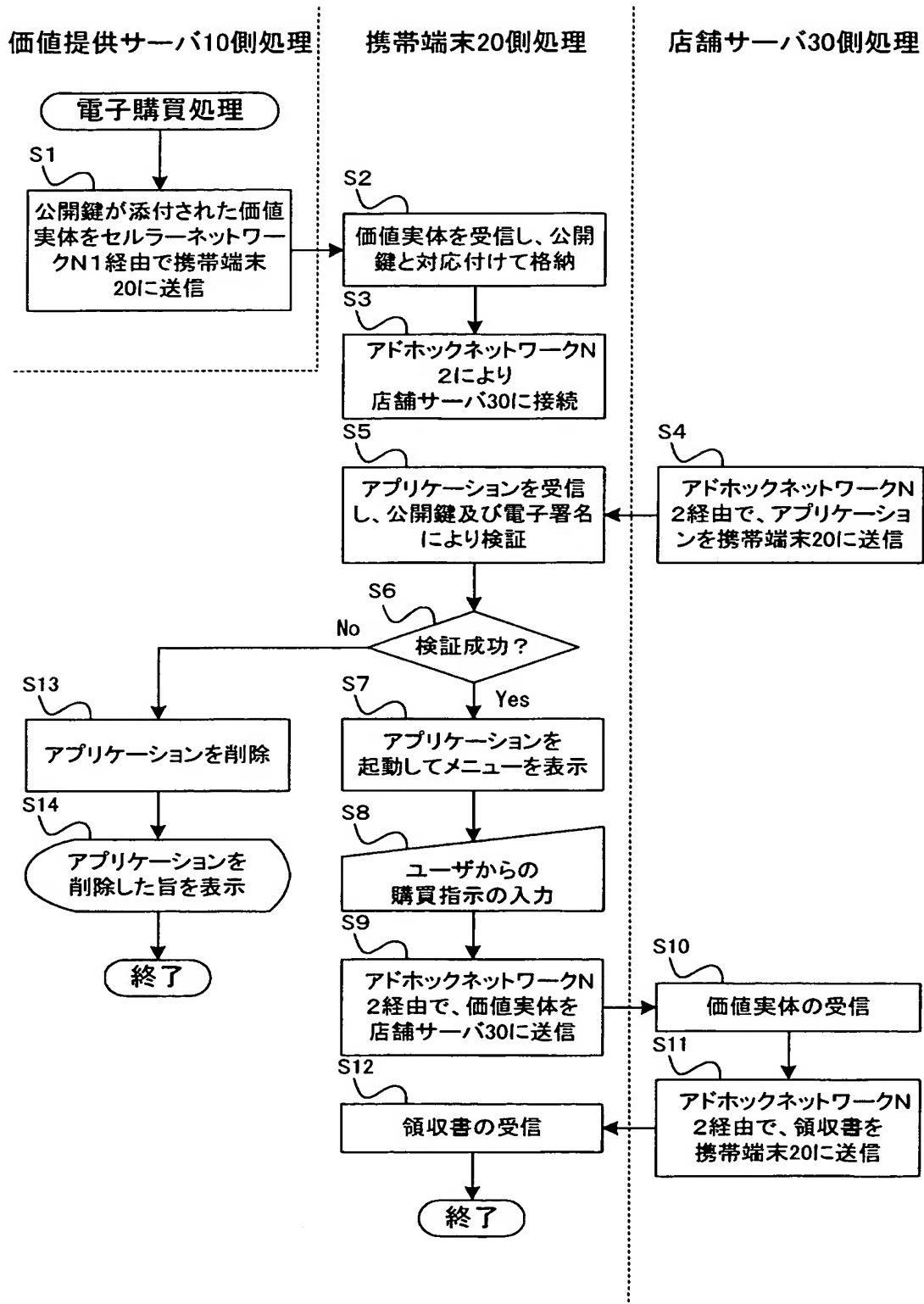


【図 3】





【図 4】



【図 5】

22

221

222

価値実体領域	サービス識別子領域
公開鍵A1が添付された 価値実体11a	0001
公開鍵A2が添付された 価値実体	0001
公開鍵A3が添付された 価値実体	0002
公開鍵A4が添付された 価値実体	0003
⋮	⋮

【図 6】

表示装置

20d

201

201a

コーヒーショップメニュー

＊ ＊ 当店のお薦め ＊ ＊

☒ ドライカフェラテ 350円

＊ ＊ 本日のコーヒー ＊ ＊

☐ フレンチロースト 300円

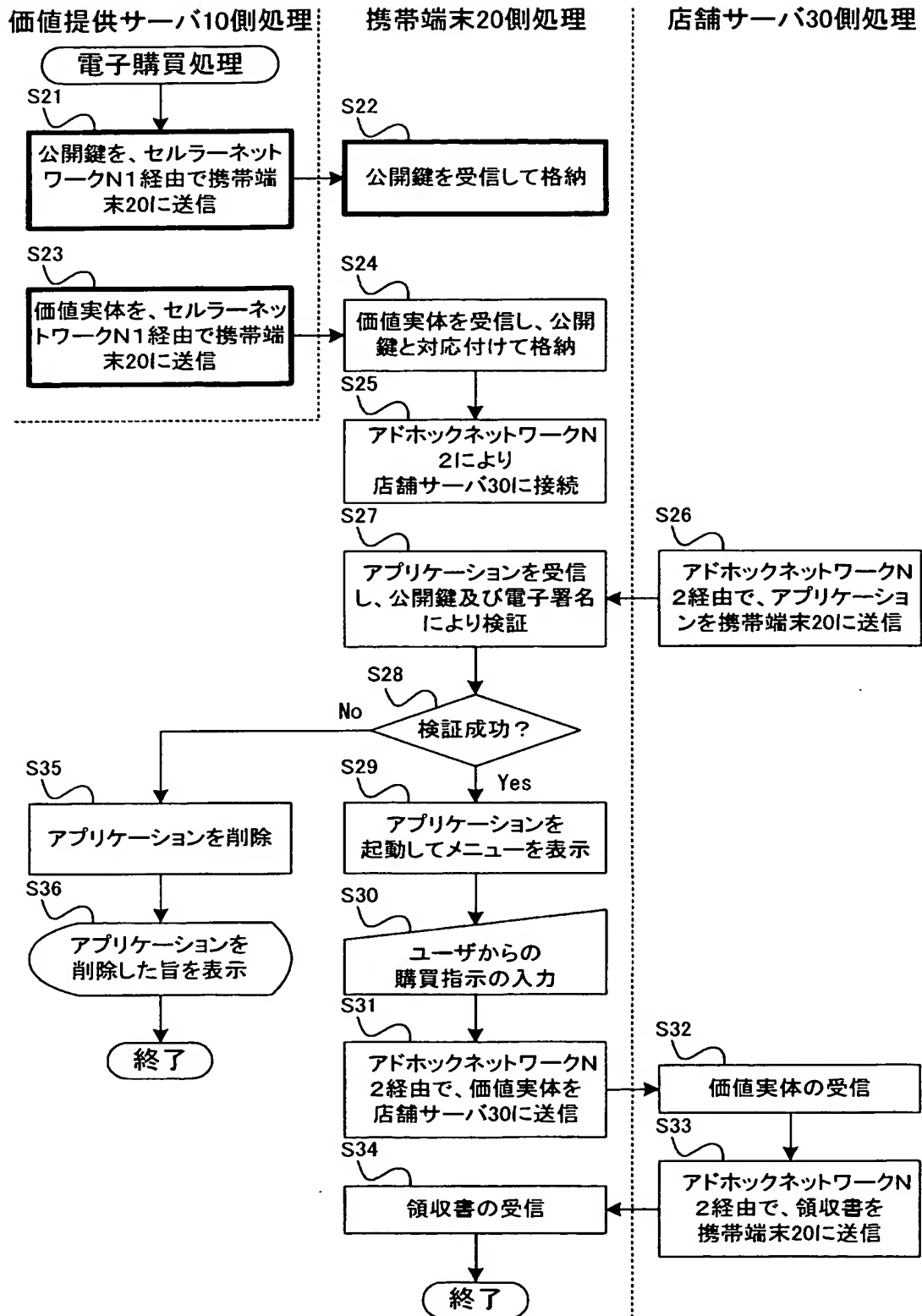
――メニュー――

☐ エスプレッソ 300円

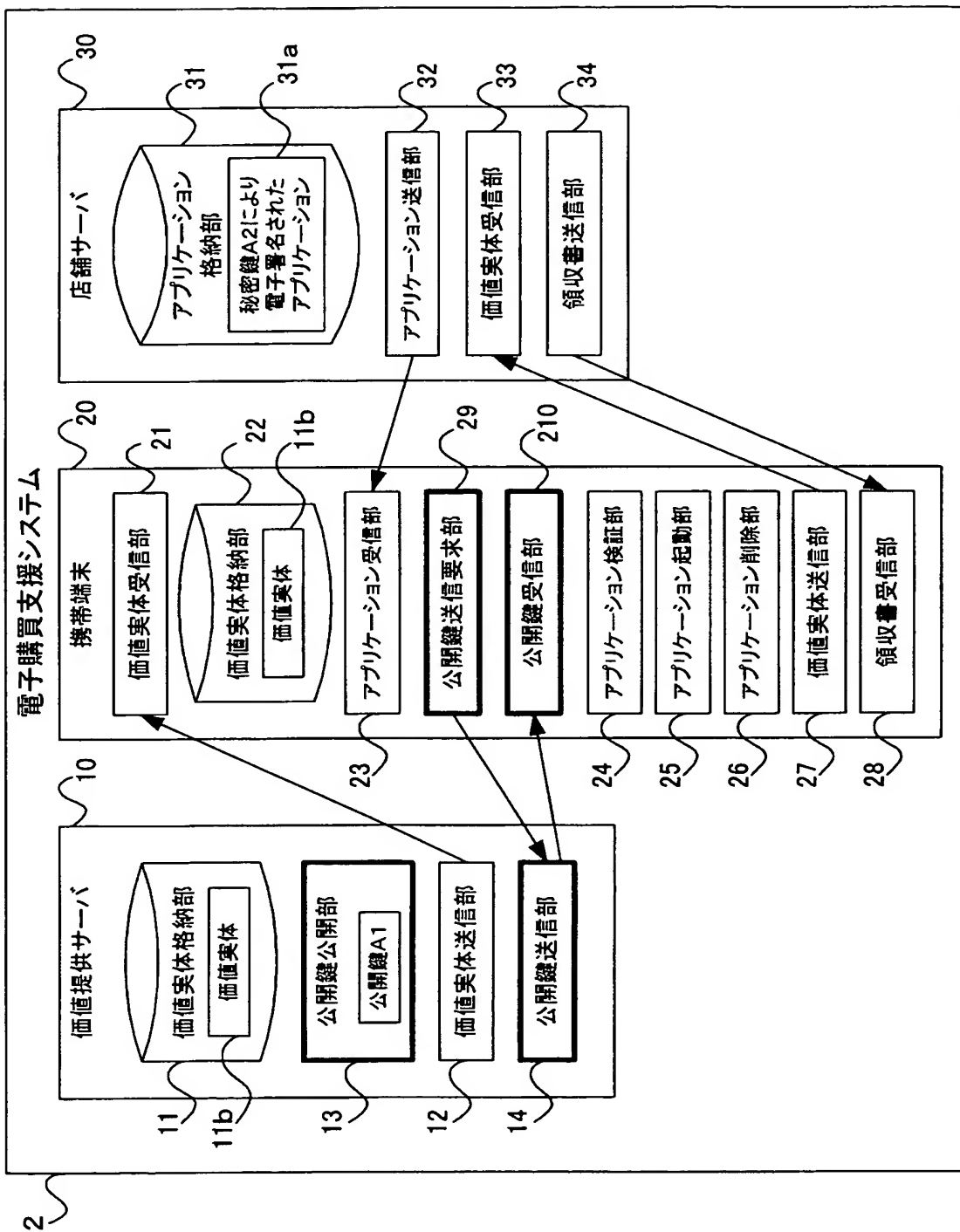
☐ カプチーノ 400円

☐ アイスコーヒー 400円

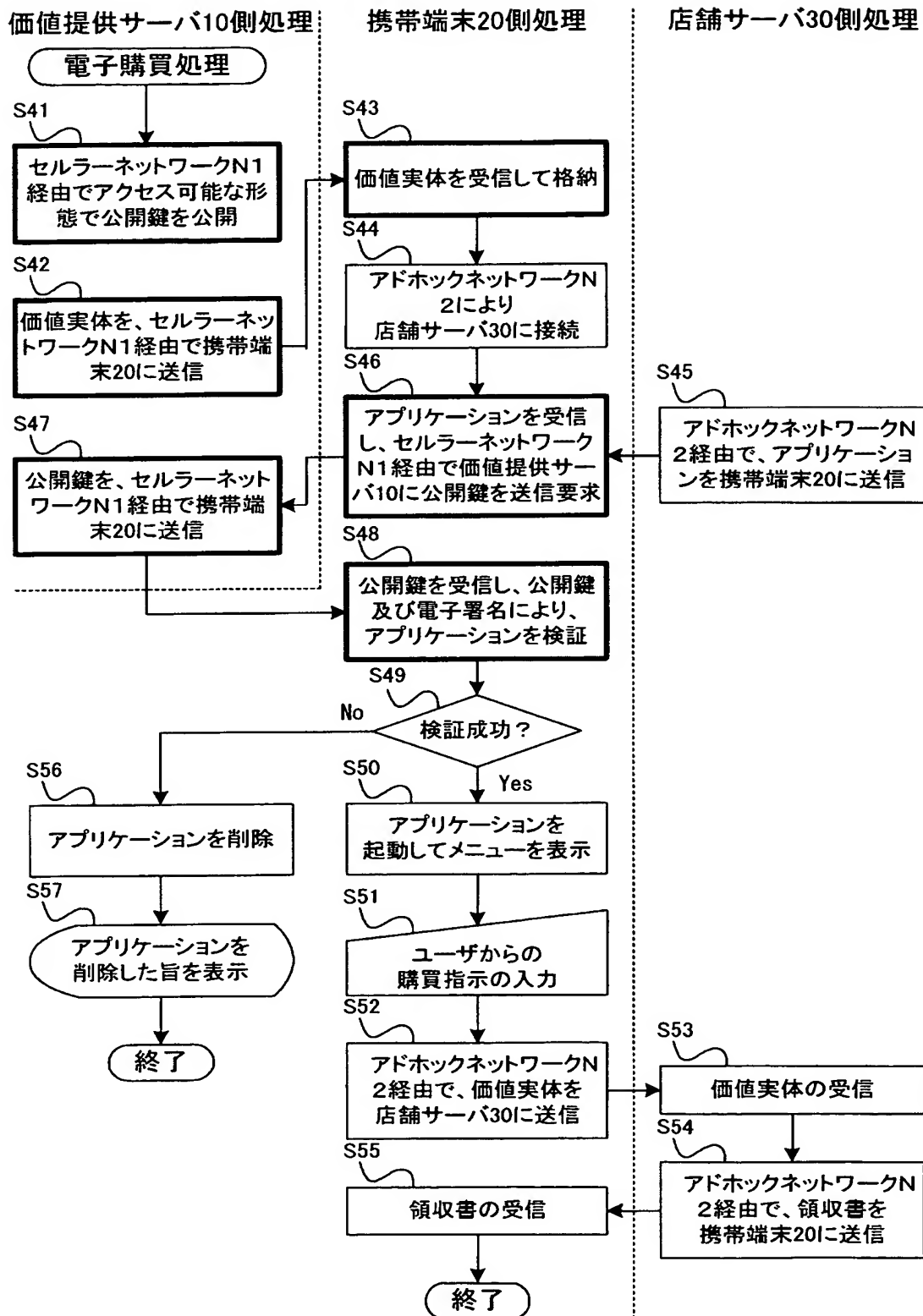
【図 7】



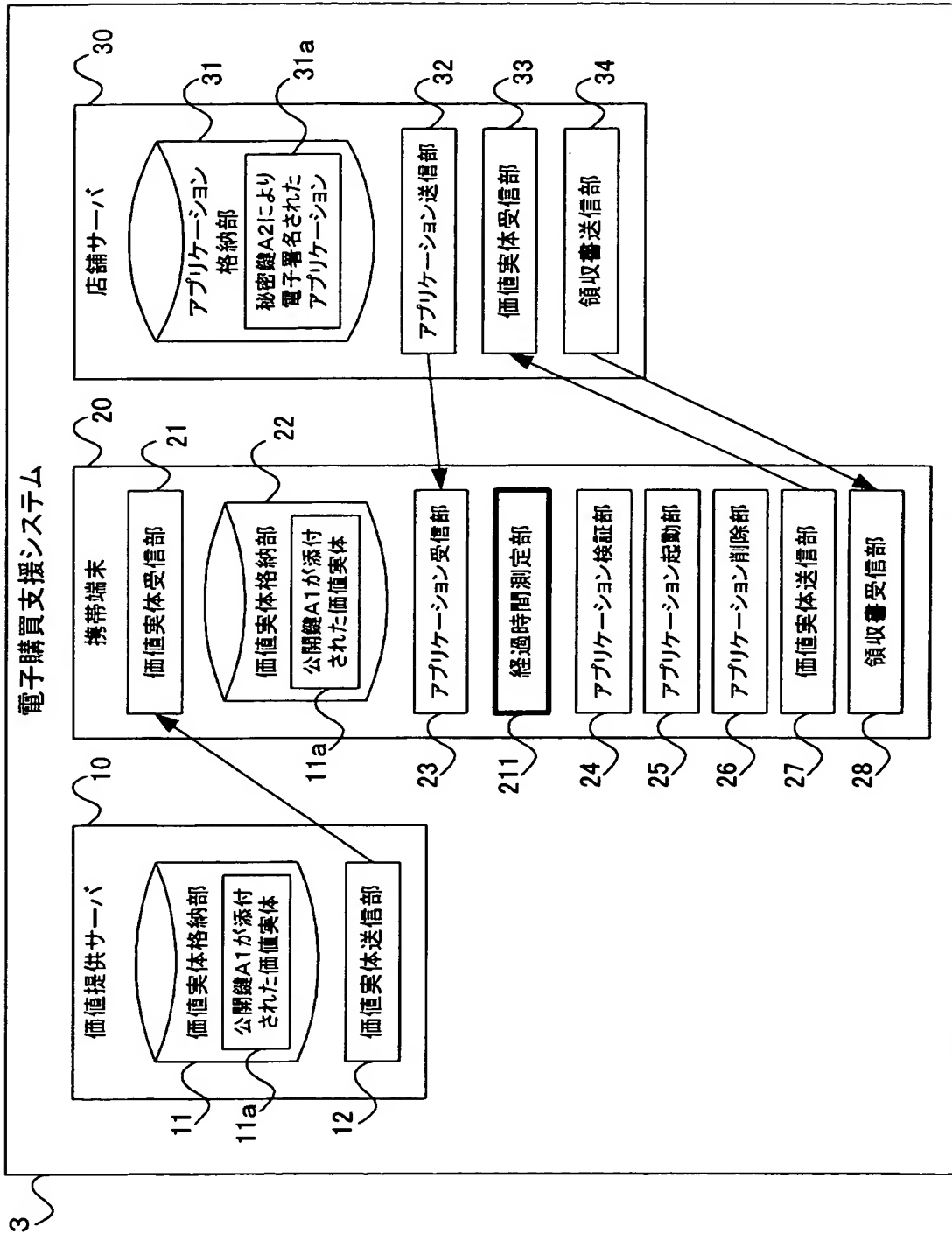
【図 8】



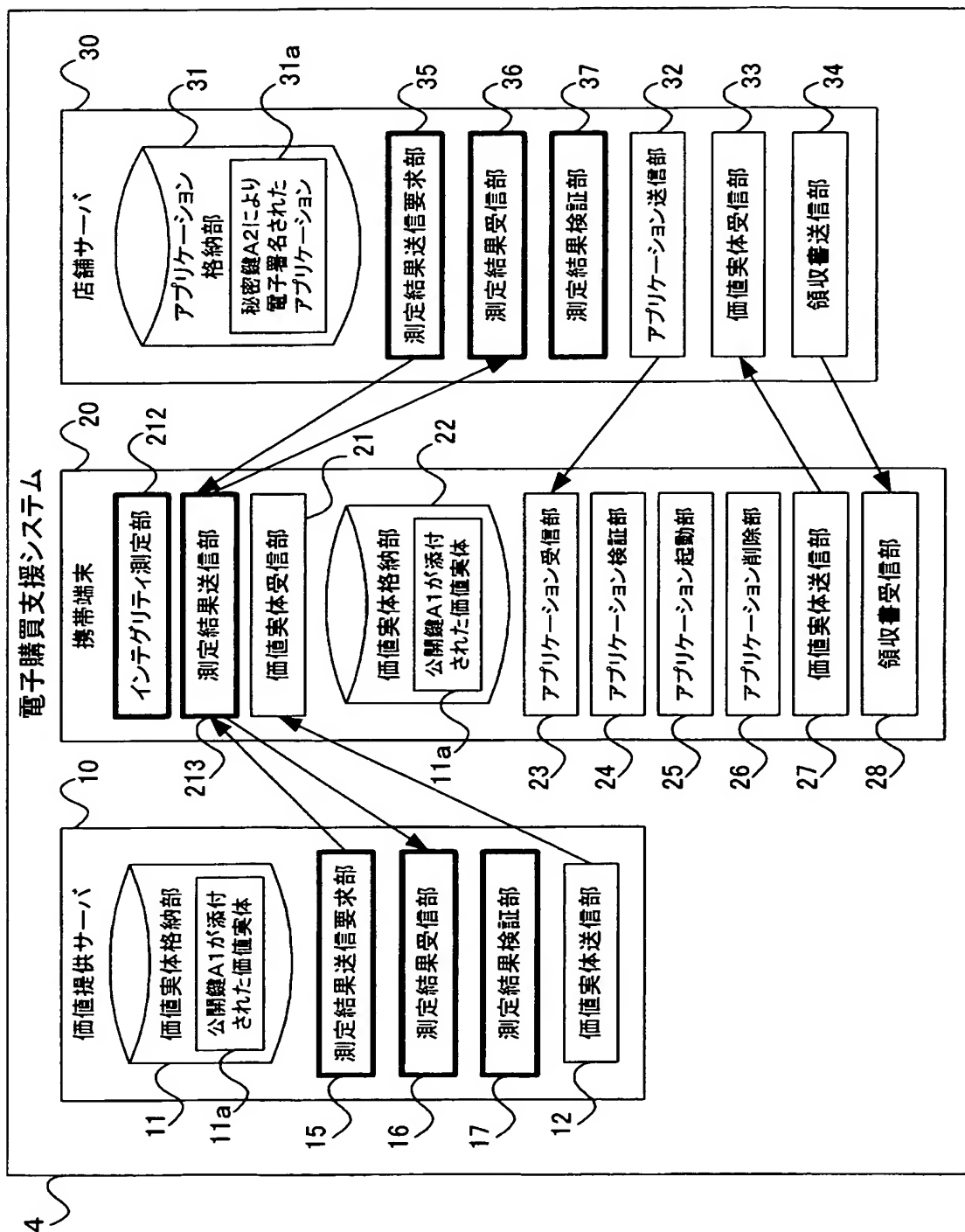
【図 9】



【図 10】

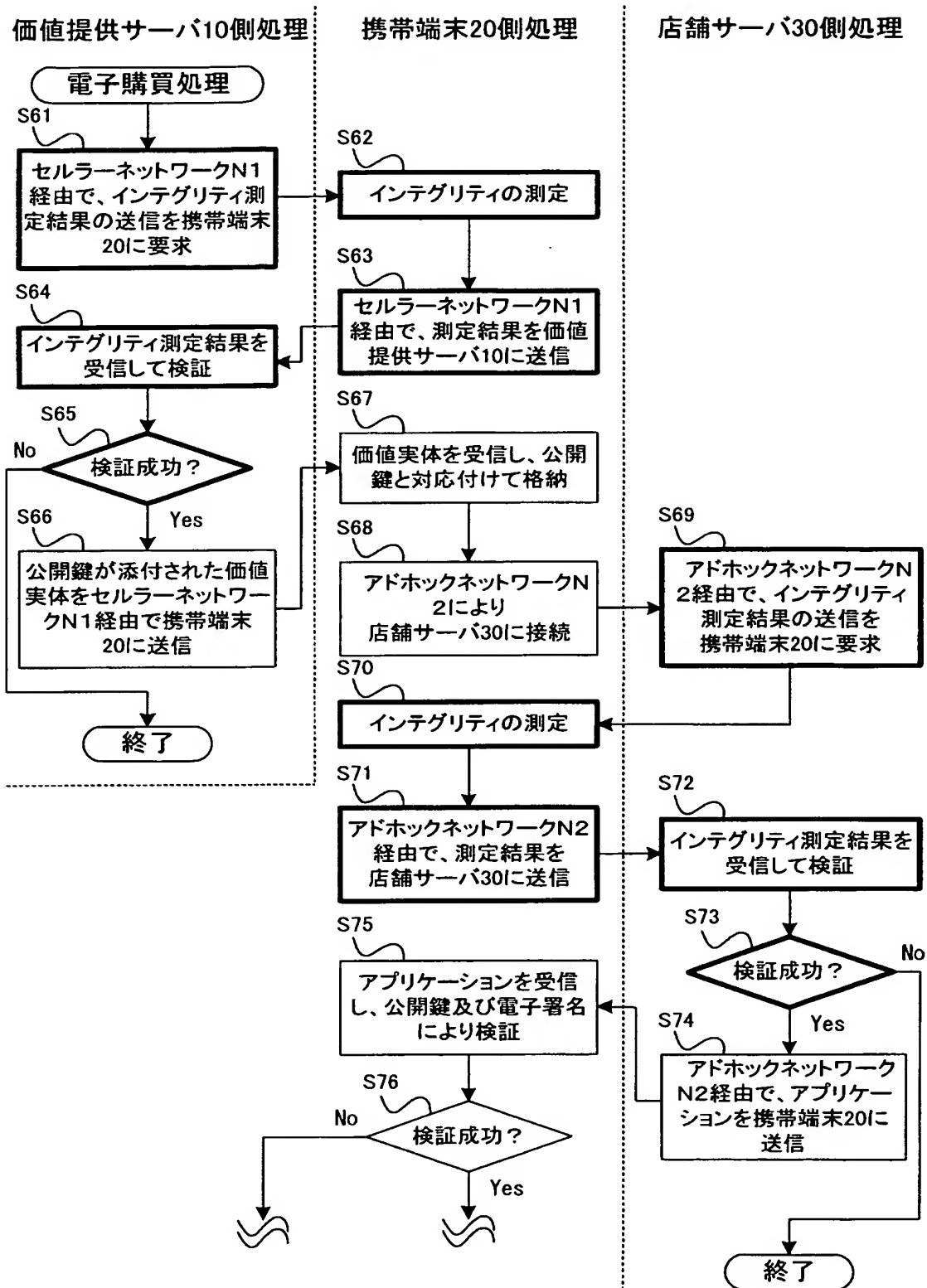


【図 11】

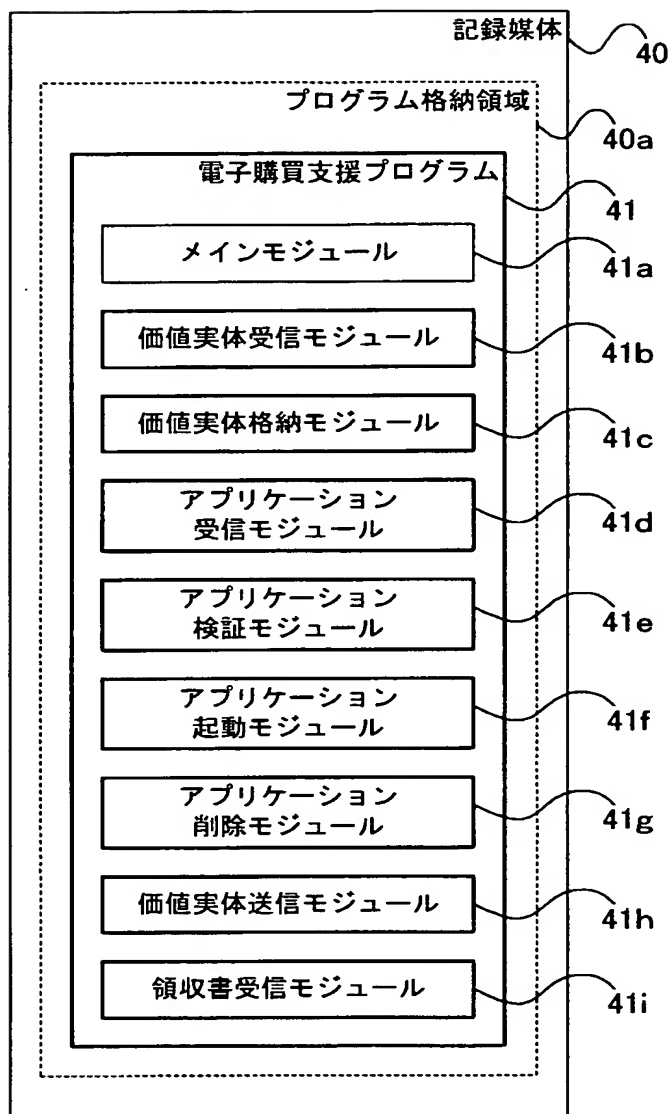




【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことである。

【解決手段】 本発明に係る携帯端末 20 は、価値実体受信部 21 と、アプリケーション受信部 23 と、アプリケーション検証部 24 と、価値実体送信部 27 とを備える。価値実体受信部 21 は、秘密鍵 A2 に対応する公開鍵 A1 が添付された価値実体 11a を受信し、受信された価値実体 11a は価値実体格納部 22 に格納される。アプリケーション受信部 23 は、秘密鍵 A2 によって電子署名されたアプリケーション 31a をアドホックネットワーク N2 経由で受信する。アプリケーション検証部 24 は、公開鍵 A1 を使用してアプリケーション 31a を検証し、検証が成功した場合には、価値実体送信部 27 は、アプリケーション 31a を使用して価値実体 11a を店舗サーバ 30 宛に送信（移転）する。

【選択図】 図 2



特願 2 0 0 2 - 3 3 8 5 5 8

出 願 人 履 歴 情 報

識別番号

[ 3 9 2 0 2 6 6 9 3 ]

1. 変更年月日  
[変更理由]

2 0 0 0 年 5 月 1 9 日

名称変更

住所変更

住 所  
氏 名

東京都千代田区永田町二丁目 1 1 番 1 号  
株式会社エヌ・ティ・ティ・ドコモ